VideoJet X20

Network Video Server

BOSCH

en Installation and Operating Manual

Table of Contents

1	**Preface**	**7**
1.1	About this Manual	7
1.2	Conventions in this Manual	7
1.3	Intended Use	7
1.4	EU Directives	8
1.5	Rating Plate	8
2	**Safety Information**	**9**
2.1	Electric Shock Hazard	9
2.2	Installation and Operation	9
2.3	Maintenance and Repair	9
3	**Product Description**	**11**
3.1	Scope of Delivery	11
3.2	System Requirements	12
3.3	Overview of Functions	13
3.4	Connections on the Front Panel	16
3.5	Connections on the Rear Panel	17
4	**Installation**	**19**
4.1	Preparations	19
4.2	Mounting	19
4.3	Connections	20
4.4	Power On/Power Off	25
4.5	Setup Using the Configuration Manager	25
5	**Configuration Using a Web Browser**	**27**
5.1	Connecting	27
5.2	Configuration Menu	29
5.3	Identification	31
5.4	Camera Names	31
5.5	Display Stamping	32
5.6	Password	34
5.7	Language	35
5.8	Date/Time	35
5.9	Time Server	35
5.10	Picture Settings	37
5.11	Encoder Profile	38
5.12	Profile Configuration	40
5.13	Video Input	43
5.14	Audio	44
5.15	JPEG Posting	45
5.16	Storage Medium	47
5.17	iSCSI	48
5.18	Partitioning	51

5.19	Recording Profiles	56
5.20	Recording Scheduler	58
5.21	Alarm Sources	60
5.22	Alarm Connections	61
5.23	VCA	64
5.24	Alarm E-Mail	69
5.25	Alarm Task Editor	71
5.26	Relay Settings	72
5.27	COM1	74
5.28	Network	76
5.29	Multicasting	80
5.30	Encryption	82
5.31	Version Information	84
5.32	Livepage Configuration	85
5.33	System State	88
5.34	Licenses	88
5.35	Maintenance	89
5.36	Function Test	91
6	**Operation**	**93**
6.1	Operation with Microsoft Internet Explorer	93
6.2	The LIVEPAGE	95
6.3	Saving Snapshots	98
6.4	Recording Video Sequences	98
6.5	Running Recording Program	99
6.6	The RECORDINGS Page	100
6.7	Backup	103
6.8	Installing the Player	104
6.9	Hardware Connections Between Video Servers	105
6.10	Operation Using Software Decoders	107
7	**Maintenance and Upgrades**	**109**
7.1	Testing the Network Connection	109
7.2	Unit Reset	109
7.3	Repairs	110
7.4	Transfer and Disposal	110
8	**Appendix**	**111**
8.1	Troubleshooting	111
8.2	General Malfunctions	112
8.3	Malfunctions with iSCSI Connections	113
8.4	LEDs	114
8.5	Processor Load	115
8.6	Serial Interface	115
8.7	Terminal Block	116
8.8	Communication with Terminal Program	117
9	**Glossary**	**119**

10 Specifications 123
10.1 Unit 123
10.2 Protocols/Standards 124

11 Index 125

1 Preface

1.1 About this Manual

This manual is intended for persons responsible for the installation and operation of the VideoJet X20. International, national and any regional electrical engineering regulations must be followed at all times. Relevant knowledge of network technology is required. The manual describes the installation and operation of the unit.

1.2 Conventions in this Manual

In this manual, the following symbols and notations are used to draw attention to special situations:

CAUTION!
This symbol indicates that failure to follow the safety instructions described may endanger persons and cause damage to the unit or other equipment.
It is associated with immediate, direct hazards.

NOTICE!
This symbol refers to features and indicates tips and information for easier, more convenient use of the unit.

1.3 Intended Use

The VideoJet X20 network video server transfers video, audio and control signals over data networks (Ethernet LAN, Internet). There are various memory options for recording the images captured by the connected camera. The unit is intended for use with CCTV systems. Various functions can be triggered automatically by incorporating external alarm sensors. Other applications are not permitted.
In the event of questions concerning the use of the unit which are not answered in this manual, please contact your sales partner or:
Bosch Sicherheitssysteme GmbH
Robert-Koch-Straße 100
85521 Ottobrunn
Germany
www.bosch-sicherheitssysteme.de

1.4 EU Directives

The VideoJet X20 network video server complies with the requirements of EU Directives 89/336 (Electromagnetic Compatibility) and 73/23, amended by 93/68 (Low Voltage Directive).

1.5 Rating Plate

For exact identification, the model name and serial number are inscribed on the bottom of the housing. Please make a note of this information before installation if necessary so as to have it to hand in case of questions or when ordering spare parts.

2 Safety Information

2.1 Electric Shock Hazard

- Never attempt to connect the unit to any power network other than the type for which it is intended.
- Use only power supply units with UL approval and a power output according to LPS or NEC Class 2.
- Never open the housing.
- Never open the housing of the power supply unit.
- If a fault occurs, disconnect the power supply unit from the power supply and from all other units.
- Install the power supply and the unit only in a dry, weather-protected location.
- If safe operation of the unit cannot be ensured, remove it from service and secure it to prevent unauthorized operation. In such cases, have the unit checked by Bosch Security Systems.

  Safe operation is no longer possible in the following cases:
  - if there is visible damage to the unit or power cables,
  - if the unit no longer operates correctly,
  - if the unit has been exposed to rain or moisture,
  - if foreign bodies have penetrated the unit,
  - after long storage under adverse conditions, or
  - after exposure to extreme stress in transit.

2.2 Installation and Operation

- The relevant electrical engineering regulations and guidelines must be complied with at all times during installation.
- Relevant knowledge of network technology is required to install the unit.
- Before installing or operating the unit, make sure you have read and understood the documentation for the other equipment connected to it, such as cameras. The documentation contains important safety instructions and information about permitted uses.
- Perform only the installation and operation steps described in this manual. Any other actions may lead to personal injury, damage to property or damage to the equipment.

2.3 Maintenance and Repair

- Never open the housing of the VideoJet X20. The unit does not contain any user-serviceable parts.
- Never open the housing of the power supply unit. The power supply unit does not contain any user-serviceable parts.
- Ensure that all maintenance or repair work is carried out only by qualified personnel (electrical engineers or network technology specialists).

3 Product Description

3.1 Scope of Delivery

- VideoJet X20 network video server (with or without integrated hard drive)
- 4 terminal blocks
- Drilling template
- Quick Installation Guide
- Product CD with the following content:
  - Quick Installation Guide
  - Manual
  - System Requirements document
  - Further documentation on Bosch Security Systems products
  - Configuration Manager
  - MPEG ActiveX control
  - Player and Archive Player
  - DirectX control
  - Microsoft Internet Explorer
  - Sun JVM
  - Adobe Acrobat Reader

NOTICE!
Check that the delivery is complete and in perfect condition. Have your unit checked by Bosch Security Systems if you detect any damage.

3.2 System Requirements

3.2.1 General Requirements

- Computer with Windows 2000 or Windows XP operating system
- Network access (Intranet or Internet)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

3.2.2 Additional Configuration Requirements

- Microsoft Internet Explorer (version 6.0 or higher)
  or
- Installed Configuration Manager program (version 1.60 or higher)

3.2.3 Additional Operational Requirements

- Microsoft Internet Explorer (version 6.0 or higher)
  or
- Receiver software, for example VIDOS (version 3.11 or higher) or Bosch Video Management System
  or
- MPEG-4 compatible hardware decoder from Bosch Security Systems (for example VIP XD) as a receiver and connected video monitor
- For playing back recordings: connection to storage medium

3.3 Overview of Functions

3.3.1 Network Video Server

The VideoJet X20 is a compact network video server for two connected video sources. It is primarily designed for encoding video, audio and control data for transfer over an IP network. With its encoding in the MPEG-4 format, the VideoJet X20 is ideally suited for making existing analog CCTV cameras IP-compatible and for remote access to digital VCRs and multiplexers. The use of existing networks means that integration with CCTV systems or local networks can be achieved quickly and easily.

Two units, a VideoJet X20 as a sender and a VIP XD as a receiver, for example, can create a standalone system for data transfer without a PC. Video images from a single sender can be received simultaneously on multiple receivers. Audio signals can also be transmitted from and to compatible units.

The VideoJet X20 features industrial standard, robust equipment and is therefore equally suited to stationary as well as mobile use in rail or other vehicles.

3.3.2 Receiver

Compatible MPEG-4 enabled hardware decoders such as VIP XD can be used as receivers. Computers with decoding software installed, such as VIDOS, or computers with the Microsoft Internet Explorer Web browser can also be used as receivers.

3.3.3 Video Encoding

The VideoJet X20 uses the MPEG-4 video compression standard. Thanks to efficient encoding, the data rate remains low even with high image quality and can also be adapted to local conditions within wide limits.

3.3.4 Dual Streaming

Dual Streaming allows the incoming data stream to be encoded simultaneously according to two different, individually customized profiles. This feature creates two data streams per camera that can serve different purposes, for example one for recording and one optimized for transmission over the LAN.

3.3.5 Multicast

In suitably configured networks, the multicast function enables simultaneous real-time video transmission to multiple receivers. The UDP and IGMP V2 protocols must be implemented on the network for this function.

3.3.6 Encryption

The VideoJet X20 offers a variety of options for protection against unauthorized reading. Web browser connections can be protected using HTTPS. You can protect the control channels via the SSL encryption protocol. With an additional license, the user data itself can be encrypted.

3.3.7 Remote Control

For remote control of external units such as pan or tilt heads for cameras or motorized zoom lenses, control data is transmitted via the VideoJet X20's bidirectional serial interface. This interface can also be used to transmit transparent data.

3.3.8 Tamper Detection and Motion Detectors

The VideoJet X20 offers a wide range of configuration options for alarm signaling in the event of tampering with the connected cameras. An algorithm for detecting movement in the video image is also part of the scope of delivery and can optionally be extended to include special video analysis algorithms.

3.3.9 Snapshots

Individual video images (snapshots) can be called up from the VideoJet X20, stored on the computer's hard drive or displayed in a separate browser window in JPEG format.

3.3.10 Recordings

Various local memory options enable the VideoJet X20 to be used as a digital VCR. The VideoJet X20 supports ANR technology, which guarantees seamless recording without gaps via VIDOS-NVR, even during network failures. A connection to an appropriately configured iSCSI system enables long-term recordings with high image quality over the network.

3.3.11 Backup

A function for storing the video images displayed on the hard drive of your computer is available on the LIVEPAGE as well as on the RECORDINGS page. Video sequences can be stored by means of a mouse click and can be redisplayed using the Player supplied as part of the scope of delivery.

3.3.12 Integrated Network Switch

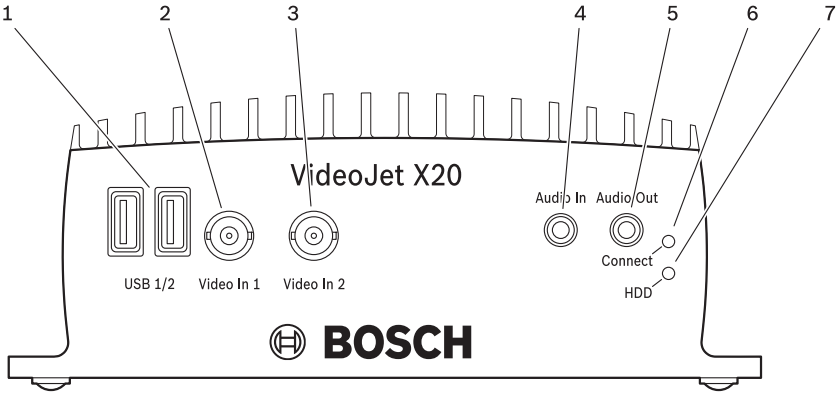
The integrated switch functionality of the VideoJet X20 permits the ETH 1, ETH 2 and SFP interfaces to be used alternatively, redundantly or for cascading other units.

3.3.13 Summary

The VideoJet X20 offers the following main functions:

- Video and data transmission over IP data networks
- Dual Streaming function for the encoder for simultaneous encoding with two individually definable profiles
- Multicast function for simultaneous image transmission to multiple receivers
- Two analog BNC composite video inputs (PAL/NTSC)
- Video encoding to international standard MPEG-4
- Two redundant integrated Ethernet ports (10/100 Base-T)
- SFP slot for mini-GBIC modules (1 Gbps)
- Integrated switch functionality
- CF slot for CompactFlash cards of up to 8 GB for local storage
- Optional, integrated robust hard drive for local storage
- USB interfaces for future WAN or WLAN connections
- Transparent, bidirectional data channel via RS232/RS422/RS485 serial interface
- Configuration and remote control of all internal functions via TCP/IP, also secured via HTTPS
- Password protection to prevent unauthorized connection or configuration changes
- Extensive, flexible storage options
- Four alarm inputs and four relay outputs
- Built-in video sensor for motion and tamper alarms
- Event-controlled automatic connection
- Convenient maintenance via uploads
- Flexible encryption of control and data channels
- Authentication according to international standard 802.1x
- Transmission and receipt of audio signals
- Bidirectional audio (mono) for line connections
- Audio encoding to international standard G.711

3.4 Connections on the Front Panel



1 **USB 1/2** interfaces
for future expansion of functions

2 **Video In 1** video input
BNC socket for connecting the first video source

3 **Video In 2** video input
BNC socket for connecting the second video source

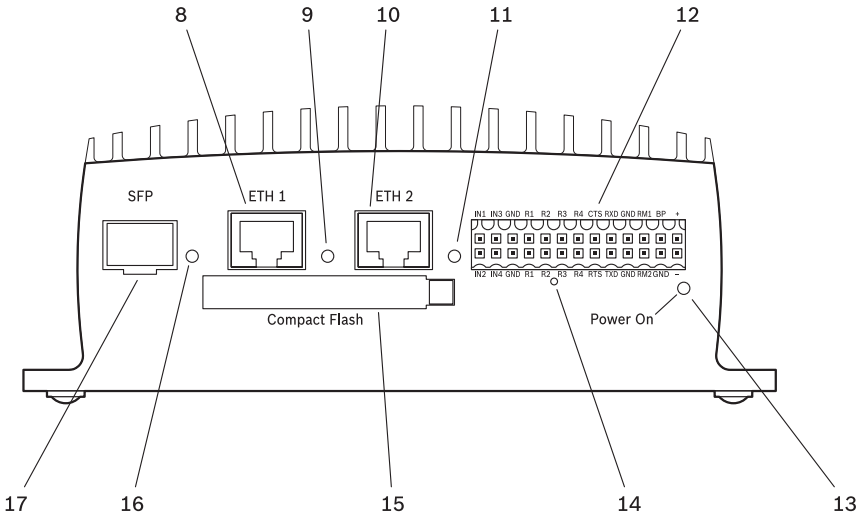
4 **Audio In** audio line input
3.5 mm stereo socket for connecting two audio line input signals

5 **Audio Out** audio line output
3.5 mm stereo socket for connecting an audio line output signal

6 **Connect** LED
flashes green when the unit is connected to a video

7 **HDD** LED
flashes orange when hard drive activity is detected
(only on units with a hard drive installed)

3.5 Connections on the Rear Panel



8 **ETH 1** RJ45 socket
for connecting to an Ethernet LAN (local network), 10/100 MBit Base-T

9 **ETH 1** LED
lights up yellow when the unit is connected to the network via **ETH 1**

10 **ETH 2** RJ45 socket
for a redundant connection to the network or to an iSCSI system

11 **ETH 2** LED
lights up yellow when the unit is connected to the network via **ETH 2**

12 Terminal block
for alarm inputs, relay outputs, serial interface and power supply

13 **Power On** LED
lights up green when ready for operation

14 Factory reset button
to restore factory default settings

15 **Compact Flash** slot
for a CF card type I or type II

16 **SFP** LED
lights up yellow when the unit is connected via **SFP**

17 **SFP** slot
for mini-GBIC module

NOTICE!
For more information about the LEDs, see *Section 8.4 LEDs*, page 114.
For terminal block assignment, see *Section 8.7 Terminal Block*, page 116.

4 Installation

4.1 Preparations

The VideoJet X20 features industrial standard equipment and is therefore suitable for both stationary installation and mobile installation in vehicles.

CAUTION!
The unit is intended for use indoors or in housings.
Select a suitable location for installation that guarantees to meet the environmental conditions. The ambient temperature must be between –30 and +60 °C (–22 and +140 °F).
The relative humidity must not exceed 95%.
The VideoJet X20 generates heat during operation, so you should ensure that there is adequate ventilation and enough clearance between the unit and heat-sensitive objects or equipment.

Please ensure the following installation conditions:

- Do not install the unit close to heaters or other heat sources. Avoid locations exposed to direct sunlight.
- Allow sufficient space for running cables.
- Ensure that the unit has adequate ventilation.
- When making connections, use only the cables supplied or use appropriate cables immune to electromagnetic interference.
- Position and run all cables so that they are protected from damage, and provide adequate cable strain relief where needed.
- Avoid impacts, blows and severe vibrations that exceed the specification limits (see *Section 10 Specifications*, page 123), as these can irreparably damage the unit.

4.2 Mounting

The VideoJet X20 can be permanently mounted to walls, below ceilings or other load-bearing locations using the four drillings in the unit's base.

CAUTION!
The front panel of the VideoJet X20 (video inputs) must not be pointing upwards, as internal heat dissipation is not guaranteed in this position. All other installation positions are permitted.
Make sure that the mounting location (for example wall or ceiling) can reliably hold the unit. The load bearing capacity must be adequate for four times the weight of the unit.
For mounting on metal, use screws with the following minimum specification:
M4 × 8, 8.8, DIN ISO 4017.
For mounting on concrete, use screws with the following minimum specification:
M4 × 40 mm (1.57 in) and 6 mm (0.23 in) plastic dowels, for example fischer S4, type 50106.

4.3 Connections

4.3.1 Cameras

You can connect two video sources to the VideoJet X20. Any cameras and other video sources that produce a standard PAL or NTSC signal are suitable.

1. Connect the cameras or other video sources to the BNC sockets **Video In 1** and **Video In 2** using a video cable (75 Ohm, BNC plug) .
2. If the video signal is not looped through, termination is performed by a software setting if necessary (see *Section 5.13 Video Input*, page 43).

4.3.2 Audio Connections

The VideoJet X20 has two audio ports for audio line signals.
The audio signals are transmitted two-way and in sync with the video signals. As a result, you can connect a speaker or door intercom system at the destination point, for example. The following specifications should be complied with in all cases.

2 × **Line In**:	Impedance 9 kOhm typ., 5.5 V_{p-p} max. input voltage
1 × **Line Out**:	Impedance 10 kOhm typ., 3.0 V_{p-p} max. output voltage, impedance 16 Ohm min., 1.7 V_{p-p} max. output voltage

The stereo plugs must be connected as follows:

Contact	**Line In function**	**Line Out function**
Tip	Channel 1 (camera 1)	Channel 1 (camera 1)
Middle ring	Channel 2 (camera 2)	–
Lower ring	Ground	Ground

1. Connect two audio sources with line level to the **Audio In** socket of the VideoJet X20 with a 3.5 mm stereo plug.
2. Connect a unit with line-in connection to the **Audio Out** socket of the VideoJet X20 with a 3.5 mm stereo plug.

4.3.3 Network

You can connect the VideoJet X20 to a 10/100 Base-T network using a standard UTP category 5 cable with RJ45 plugs. The second Ethernet interface can be used to create a redundant connection to the network.

NOTICE!
You cannot create a connection to a second network.

1. Connect the VideoJet X20 to the network via the **ETH 1** socket.
2. Connect the VideoJet X20 to a redundant switch or hub on the same network via the **ETH 2** socket.

4.3.4 SFP Slot

You can establish an additional network connection by inserting a mini-GBIC module into the SFP slot for example via fiber optic cables (OF).

CAUTION!
Only laser class 1 transceivers are approved for use in the VideoJet X20.
Use only approved modules.

4.3.5 Direct iSCSI Connection

You can connect the VideoJet X20 directly to an iSCSI system via one of the network interfaces. For **ETH 1** or **ETH 2** connections, use a UTP category 5 network cable with RJ45 plugs.

NOTICE!
You can obtain a list of compatible iSCSI systems from your supplier or directly from Bosch Security Systems. This list is constantly being updated and extended.

4.3.6 CF Slot

You can insert a type I or II CompactFlash card into the **Compact Flash** slot to enable recordings to be saved locally. CF cards are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions.
The VideoJet X20 supports high-performance CF cards with a storage capacity of up to 8 GB.

NOTICE!
You can obtain a list of compatible CF cards from your supplier or directly from Bosch Security Systems. This list is constantly being updated and extended.

Playing back recordings is also possible using a different VideoJet X20 or a VideoJet X40.

CAUTION!
Setting up partitions clears all existing data from the card.
You should therefore check whether the CF card contains any data that needs to be backed up before it is inserted.

1. Carefully slide the CF card, top side down, into the slot as far as it will go.
2. To remove the CF card, push the eject button to its right and then take out the card.

4.3.7 Data Interface

The bidirectional data interface is used to control units connected to the VideoJet X20, for example a dome camera with motorized lens. The connection supports the RS232, RS422 and RS485 transmission standards.
The VideoJet X20 offers the serial interface via the orange terminal block (see *Section 8.7 Terminal Block*, page 116).
The range of controllable equipment is expanding constantly. The manufacturers of the relevant equipment provide specific information on installation and control.

CAUTION!
Please take note of the appropriate documentation when installing and operating the unit to be controlled.
The documentation contains important safety instructions and information about permitted uses.

NOTICE!
A video connection is necessary to transmit transparent data.

4.3.8 Alarm Inputs

The VideoJet X20 has four alarm inputs on the orange terminal block (see *Section 8.7 Terminal Block*, page 116). The alarm inputs are used to connect to external alarm devices such as door contacts or sensors. When configured appropriately, an alarm device can, for example, trigger the VideoJet X20 to automatically establish a connection with a remote station.
A zero potential make contact or switch can be used as the actuator.

NOTICE!
If possible, use a bounce-free contact system as the actuator.

- ▶ Connect the lines to the appropriate terminals on the orange terminal block (**IN1** to **IN4**) and check that the connection is secure.

4.3.9 Relay Outputs

The VideoJet X20 has four relay outputs for switching external units such as lamps or alarm sirens. You can operate these relay outputs manually while there is an active connection to the VideoJet X20. The outputs can also be configured to automatically activate sirens or other alarm units in response to an alarm signal. The relay outputs are also located on the orange terminal block (see *Section 8.7 Terminal Block*, page 116).

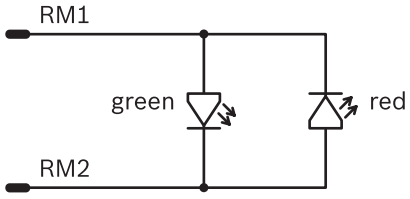
CAUTION!
A maximum load of 30 V and 2 A may be applied to the relay contacts.

▶ Connect the lines to the appropriate terminals on the orange terminal block (**R1** to **R4**) and check that the connection is secure.

4.3.10 Remote Indication of the Connection Status

When the VideoJet X20 is connected to a video, the **Connect** LED on the front panel of the unit flashes. The LED also provides information on the operational state of the unit and signals a unit defect (see *Section 8.4 LEDs*, page 114).
You can connect an additional two-color LED to the VideoJet X20 as a remote indicator. This provides the same information as the integrated **Connect** LED. A remote indicator can be useful if the VideoJet X20 is installed at a location that is difficult to access or see, for example in a cable duct or on top of a mast. Just like the integrated LED, the remote indicator LED should also light up red and green in order to avoid confusion.
Please comply with the following specifications and the connection diagram:

Voltage between **RM1** and **RM2**	3.3 V DC max.
Current between **RM1** and **RM2**	25 mA max.
Source resistance	140 Ohm typ.



1. Connect the LED lines to the appropriate terminals on the orange terminal block (**RM1** and **RM2**) and check that the connection is secure.
2. Check that the signals on the **Connect** LED on the VideoJet X20 and the remote indicator LED correspond.

4.3.11 Backup Power Supply

When used in mobile vehicles (for example public transport), the VideoJet X20 is usually switched on when the vehicle is started with the ignition key. If the ignition is switched off, the power supply to the unit is also stopped. To keep the internal clock running when the engine is off, you can connect the VideoJet X20 directly to the car battery via the **BP** and **GND** contacts. The correct time is crucial for evaluating local recordings.

CAUTION!
Connect only batteries with the following specification: 10 to 30 V DC, 50 Ah max., 12/24 V continuous flow.

1. Connect the **+** (plus) line on the car battery to the **BP** terminal on the orange terminal block.
2. Connect the **–** (minus) line on the car battery to the **GND** terminal on the orange terminal block.
3. Now check that the connections are secure.

4.4 Power On/Power Off

4.4.1 Power Supply

The VideoJet X20 does not have a power switch. Power is supplied via a separate unit. Connect the VideoJet X20 to the power supply unit and plug this into the mains. The unit is now ready for use. The VideoJet X20 does not come supplied with a power supply unit.

CAUTION!

Use only power supply units with UL approval and a power output according to LPS or NEC Class 2.

Where necessary, use suitable equipment to ensure that the power supply is free from interference such as voltage surges, spikes or voltage drops.

Do not connect the VideoJet X20 to the power supply until all other connections have been made.

1. Plug the terminal block with the PSU cable connected into the orange socket on the VideoJet X20.
2. Connect the power supply unit to the mains. The VideoJet X20 is ready for use as soon as the **Connect** LED changes from a red light, indicating the start-up procedure, to a green light.

If the network connection has been set up correctly, the yellow **ETH 1** or **ETH 2** LED will also light up. A flashing **ETH 1** or **ETH 2** LED signals that data packages are being transmitted over the network.

4.5 Setup Using the Configuration Manager

The **Configuration Manager** program can be found on the product CD contained in the scope of delivery. This program allows you to implement and set up new video servers in the network quickly and conveniently.

NOTICE!

Using the Configuration Manager to set all parameters in the VideoJet X20 is an alternative to configuration by means of a Web browser, as described in chapter 5 of this manual.

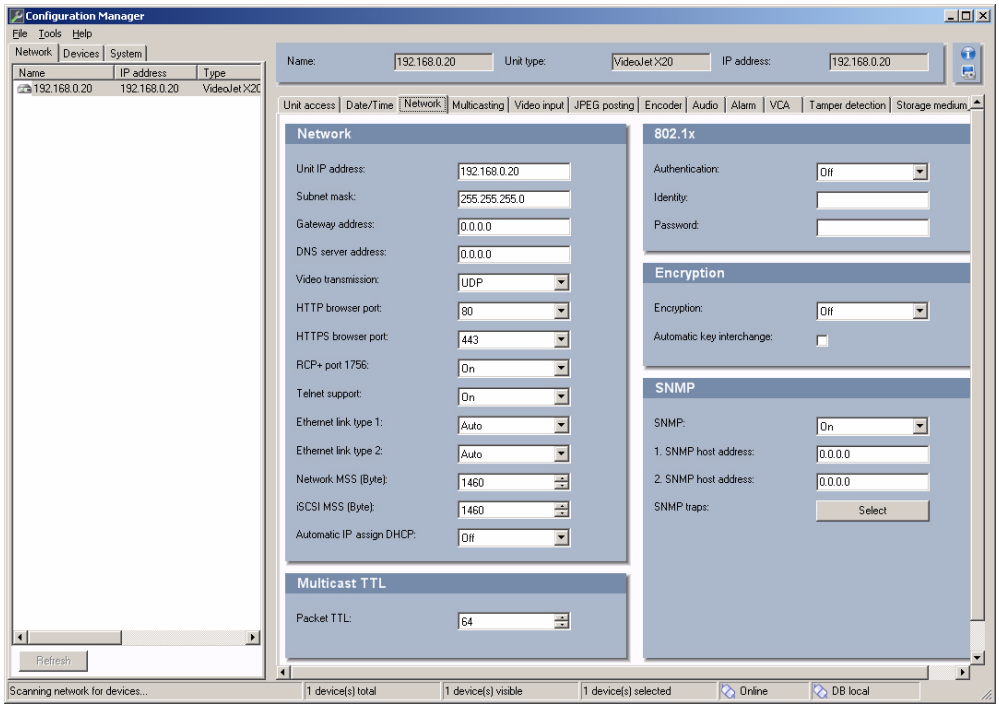
4.5.1 Installing the Program

1. Insert the CD into the computer's CD-ROM drive.
2. If the CD does not start automatically, open the **Configuration Manager** directory using Windows Explorer and double-click **Setup.exe**.
3. Follow the on-screen instructions.

4.5.2 Configuring the VideoJet X20

You can start the Configuration Manager immediately after installation.

1. Double-click the icon on the desktop or start the program via the Start menu. After the program has started, the network is immediately searched for compatible video servers.



2. You can start the configuration if a VideoJet X20 is shown in the list in the left section of the window. To do this, click the entry for the unit.
3. Click the **Network** tab in the right section of the window. The current network settings are displayed.
4. In the **Unit IP address** field, enter the required IP address (for example **192.168.0.20**) and click the **Set** button at the bottom right of the window. The new IP address is valid the next time you start the unit.
5. If required, enter a new subnet mask and additional network data.

NOTICE!
You must reboot to activate the new IP address, a new subnet mask or a gateway address.

4.5.3 Reboot

You can trigger the reboot directly with the assistance of the Configuration Manager.

▶ Right-click the entry for the unit in the list in the left section of the window and select the **Reset** command from the context menu.

4.5.4 Additional Parameters

You can check and set additional parameters with the assistance of the Configuration Manager. You can find detailed information on this in the documentation for this program.

5 Configuration Using a Web Browser

5.1 Connecting

The integrated HTTP server in the VideoJet X20 offers you the option of configuring the unit over the network with a Web browser. This option is an alternative to configuration using the Configuration Manager program and is considerably richer in function and more convenient than configuration using the terminal program.

5.1.1 System Requirements

- Computer with Windows 2000 or Windows XP operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 6.0 or higher)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

5.1.2 Installing MPEG ActiveX

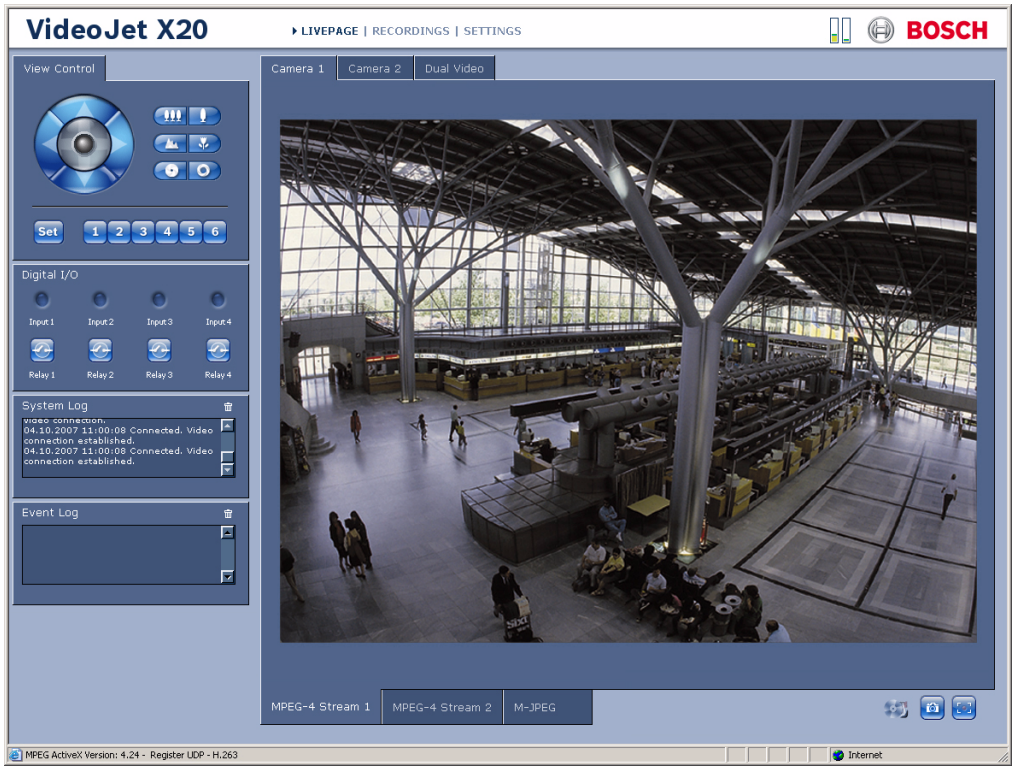
To allow the live video images to be played back, suitable MPEG ActiveX software must be installed on the computer. If necessary, you can install the program from the product CD supplied.

1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

5.1.3 Establishing the Connection

The VideoJet X20 must be assigned a valid IP address to operate on your network.
The following default address is preset at the factory: **192.168.0.1**

1. Start the Web browser.
2. Enter the VideoJet X20's IP address as the URL. The connection is established and after a short time you will see the **LIVEPAGE** with the video image.



5.1.4 Maximum Number of Connections

If you do not connect, the unit may have reached its maximum number of connections.
Depending on the unit and network configuration, each VideoJet X20 can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

5.1.5 Protected VideoJet X20

If the VideoJet X20 is password protected against unauthorized access, the Web browser displays a corresponding message and prompts you to enter the password when you attempt to access protected areas.

NOTICE!
The VideoJet X20 offers the option to limit the extent of access using various authorization levels (see *Section 5.6 Password*, page 34).

1. Enter the user name and associated password in the corresponding text fields.
2. Click **OK**. If the password is entered correctly, the Web browser displays the page that was called up.

5.1.6 Protected Network

If a RADIUS server is employed in the network for managing access rights (802.1x authentication), the VideoJet X20 must be configured accordingly, otherwise no communication is possible.
To configure the unit, you must connect the VideoJet X20 directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated (see *Section 5.28.17 Authentication*, page 79).

5.2 Configuration Menu

The **SETTINGS** page provides access to the configuration menu, which contains all the unit's parameters arranged in groups.
You can view the current settings by opening one of the configuration screens. You can change the settings by entering new values or by selecting a predefined value from a list field.
All parameter groups are described in this chapter in the order in which they are listed in the configuration menu, from the top of the screen to the bottom.

CAUTION!
The settings in the configuration menu should only be processed or modified by expert users or system support personnel.

All settings are stored in the VideoJet X20's memory so that they are retained even if the power supply is interrupted.

5.2.1 Starting Configuration

▶ Click the **SETTINGS** link in the upper section of the window. The Web browser opens a new page with the configuration menu.

5.2.2 Navigation

1. Click one of the menu items in the left window margin. The corresponding submenu is displayed.
2. Click one of the entries in the submenu. The Web browser opens the corresponding page.

5.2.3 Making Changes

Each configuration screen shows the current settings. You can change the settings by entering new values or by selecting a predefined value from a list field.

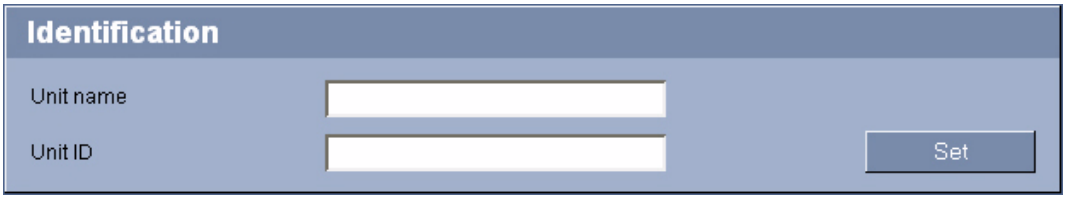
▶ After each change, click **Set** to save the change.

CAUTION!

Save each change with the associated **Set** button.

Clicking the **Set** button saves the settings only in the current field. Changes in any other fields are ignored.

5.3 Identification



5.3.1 Unit name

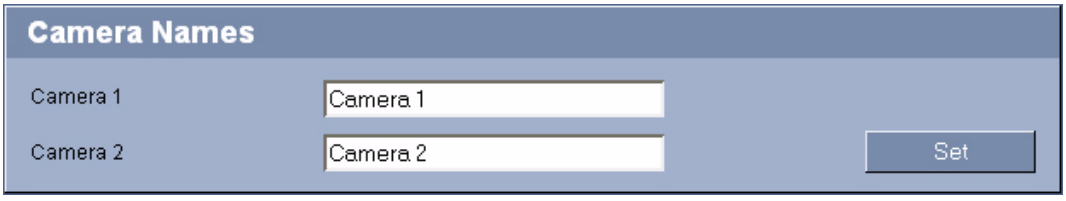
You can give the VideoJet X20 a name to make it easier to identify. The name makes the task of administering multiple units in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.
The unit name is used for the remote identification of a unit, in the event of an alarm for example. For this reason, enter a name that makes it as easy as possible to quickly identify the location.

CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player being unable to play back the recording.

5.3.2 Unit ID

Each VideoJet X20 should be assigned a unique identifier that you can enter here as an additional means of identification.

5.4 Camera Names



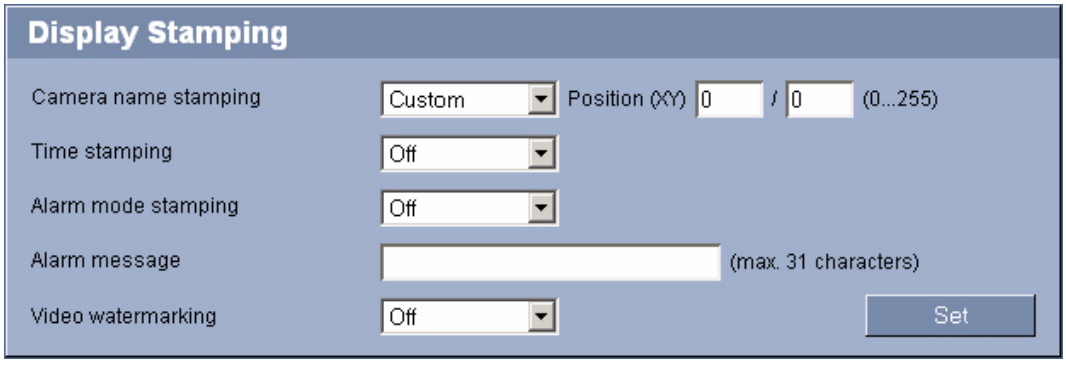
The camera name makes it easier to identify the remote camera location, in the event of an alarm for example. It will be displayed in the video screen if configured to do so (see *Section 5.5.1 Camera name stamping*, page 32). The camera name makes the task of administering cameras in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.

5.4.1 Camera 1 / Camera 2

Enter a unique, unambiguous name for the camera in this field.

CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player being unable to play back the recording.

5.5 Display Stamping



Various overlays or "stamps" in the video image provide important supplementary information. These overlays can be enabled individually and are arranged on the image in a clear manner.

NOTICE!
The settings on this page apply to both camera inputs.

5.5.1 Camera name stamping

This field sets the position of the camera name overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

5.5.2 Time stamping

This field sets the position of the time overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

5.5.3 Alarm mode stamping

Select **On** to display a text message overlay in the image in the event of an alarm. It can be displayed at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

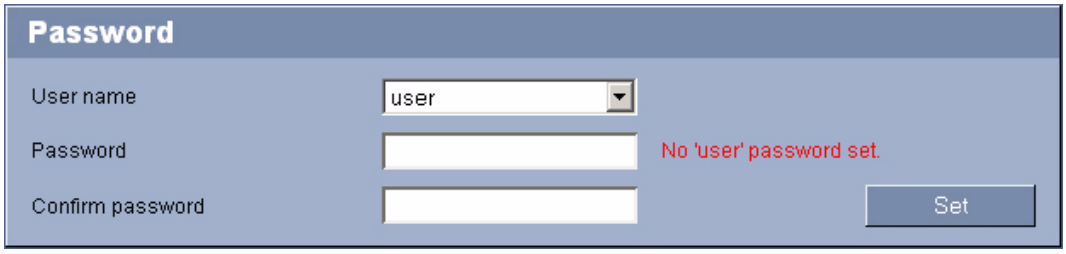
5.5.4 Alarm message

Enter the message to be displayed in the image in the event of an alarm. The maximum text length is 31 characters.

5.5.5 Video watermarking

Select **On** if you wish the transmitted video images to be "watermarked". After activation, all images are marked with a green **W**. A red **W** indicates that the sequence (live or saved) has been manipulated.

5.6 Password



A VideoJet X20 is generally protected by a password to prevent unauthorized access to the unit. You can use different authorization levels (**User name**) to limit access.

NOTICE!
Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. If a **live** password is assigned, for example, a **service** and a **user** password must also be set. When assigning passwords, you should therefore always start from the highest authorization level, **service**, and use different passwords.

5.6.1 User name

The VideoJet X20 operates with three user names: **service**, **user** and **live**, which correspond to different authorization levels.
The **service** user name is the highest authorization level. After entering the correct password, this user name allows you to use all the functions of the VideoJet X20 and change all configuration settings.
The **user** user name is the middle authorization level. You use it to operate the unit and also to control cameras, for example, but you cannot change the configuration.
The **live** user name is the lowest authorization level. It can only be used to view the live video image and switch between the different live image displays.

5.6.2 Password

You can define and change a separate password for each user name if you are logged in as **service** or if the unit is not password protected.
Enter the password for the selected user name here.

5.6.3 Confirm password

Enter the new password a second time to eliminate typing mistakes.

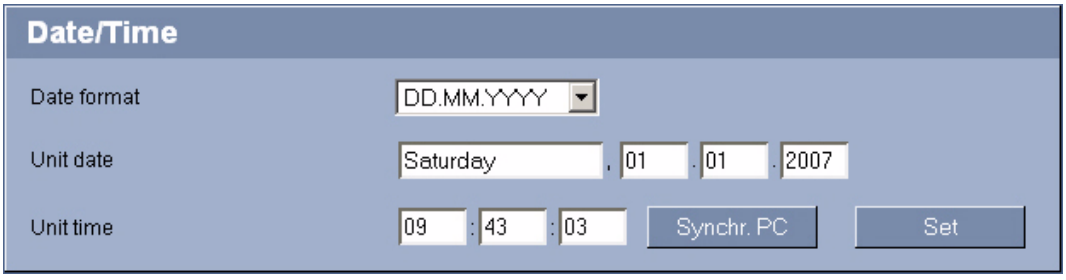
NOTICE!
The new password is only saved when you click the **Set** button. You should therefore click the **Set** button immediately after entering and confirming a password, even if you also wish to subsequently assign a password to another user name.

5.7 Language

5.7.1 Website language

Select the language for the user interface here.

5.8 Date/Time



5.8.1 Date format

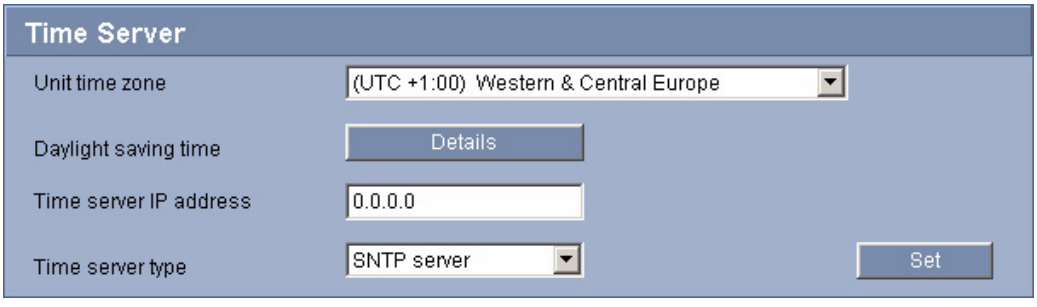
Select your required date format.

5.8.2 Unit date/Unit time

If there are multiple units operating in your system or network, it is important to synchronize their internal clocks. For example, it is only possible to identify and correctly evaluate simultaneous recordings when all units are operating on the same time.

1. Enter the current date. Since the unit time is controlled by the internal clock, there is no need to enter the day of the week — it is added automatically.
2. Enter the current time or click the **Synchr. PC** button to copy your computer's system time to the VideoJet X20.

5.9 Time Server



The VideoJet X20 can receive the time signal from a time server using various time server protocols, and then use it to set the internal clock. The unit polls the time signal automatically once every minute.

5.9.1 Unit time zone

Select the time zone in which your system is located.

5.9.2 Daylight saving time

The internal clock can switch automatically between normal and daylight saving time (DST). The unit already contains the data for DST switch-overs up to the year 2015. You can use these data or create alternative time saving data if required.

NOTICE!
If you do not create a table, there will be no automatic switching. When changing and clearing individual entries, remember that two entries are usually related to each other and dependent on one another (switching to summer time and back to normal time).

1. First check whether the correct time zone is selected. If it is not correct, select the appropriate time zone for the system, and click the **Set** button.
2. Click the **Details** button. A new window will open and you will see the empty table.
3. Select the region or the city which is closest to the system's location from the list field below the table.
4. Click the **Generate** button to generate data from the database in the unit and enter it into the table.
5. Make changes by clicking an entry in the table. The entry is selected.
6. Clicking the **Delete** button will remove the entry from the table.
7. Select other values from the list fields below the table to change the entry. Changes are made immediately.
8. If there are empty lines at the bottom of the table, for example after deletions, you can add new data by marking the row and selecting required values from the list fields.
9. Now click the **OK** button to save and activate the table.

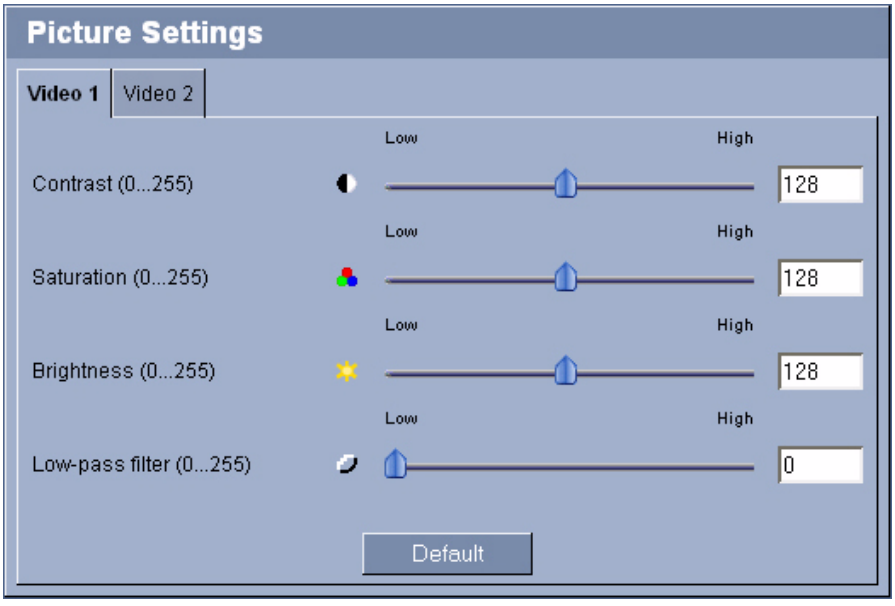
5.9.3 Time server IP address

Enter the IP address of a time server.

5.9.4 Time server type

Select the protocol that is supported by the selected time server. Preferably, you should select the **SNTP server** as the protocol. This supports a high level of accuracy and is required for special applications and subsequent function extensions.
Select **Time server** for a time server that works with the protocol RFC 868.

5.10 Picture Settings



You can set the video image of each camera to suit your requirements. The current video image is displayed in the small window next to the slide controls as confirmation. Your changes are effective immediately.

1. Click a tab to select the corresponding camera.
2. Move the slide control to the required position.
3. Click **Default** to reset all settings to their default value.

5.10.1 Contrast (0...255)

You can use this function to adapt the contrast of the video image to your working environment.

5.10.2 Saturation (0...255)

You can use this function to adjust the color saturation so as to make the reproduction of colors on your monitor as realistic as possible.

5.10.3 Brightness (0...255)

You can use this function to adapt the brightness of the video image to your working environment.

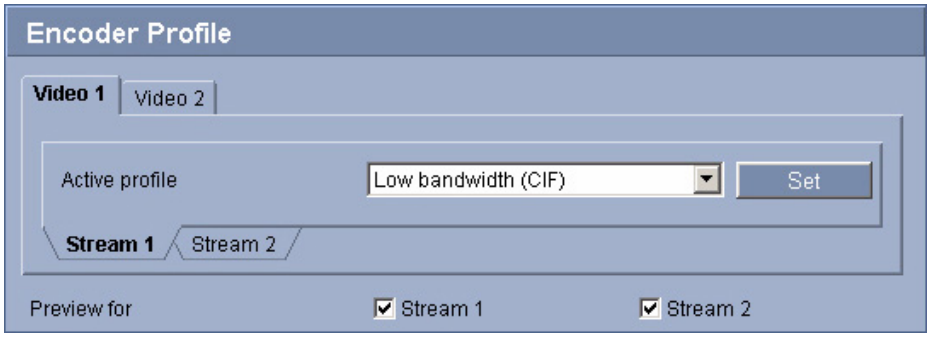
5.10.4 Low-pass filter (0...255)

You can use this function to filter very fine noise from the image. This reduces and optimizes the bandwidth necessary for image transmission over the network. The image resolution may be impaired.

The higher the value set with the slide control, the flatter the image signal. Check your setting in the image window next to the slide controls.

Also observe the processor load indicator that appears at the top of the window near the manufacturer's logo (see *Section 8.5 Processor Load*, page 115).

5.11 Encoder Profile



For encoding the video signal you can select two profiles for each encoder (video input) and change the presets for the profiles.
You can adapt the MPEG-4 data transmission to the operating environment (for example network structure, bandwidth, data load). To this end, the VideoJet X20 simultaneously generates two data streams (Dual Streaming) for each video input. You can select the compression settings of these data streams individually, for example one setting for transmissions to the Internet and one for LAN connections.

NOTICE!
You must set the parameters for each camera input and for each stream individually. The names **Video 1** and **Video 2** correspond to the labeling of the video inputs on the unit.

Pre-programmed profiles are available, each giving priority to different perspectives.

- Profile 1: **Low bandwidth (CIF)**
  High quality for low bandwidth connections,
  resolution 352 × 288/240 pixels
- Profile 2: **Low delay (2/3 D1)**
  High quality with low delay, resolution 464 × 576/480 pixels
- Profile 3: **High resolution (4CIF/D1)**
  High resolution for high bandwidth connections,
  resolution 704 × 576/480 pixels
- Profile 4: **DSL**
  For DSL connections with 500 kbps, resolution 352 × 288/240 pixels
- Profile 5: **ISDN (2B)**
  For ISDN connections via two B-channels, resolution 352 × 288/240 pixels
- Profile 6: **ISDN (1B)**
  For ISDN connections via one B-channel, resolution 352 × 288/240 pixels
- Profile 7: **Modem**
  For analog modem connections with 20 kbps, resolution 352 × 288/240 pixels
- Profile 8: **GSM**
  For GSM connections at 9,600 baud, resolution 176 × 144/120 pixels

5.11.1 Active profile

Here you can select the desired profile for each of the two streams. You will see a preview for each data stream in the right section of the window. The preview of the data stream currently selected is marked by a red frame. Above the previews, various additional items of information regarding data transmission are displayed and continually updated.

1. First, click a tab at the top to select the associated camera.
2. Click a tab at the bottom to select the associated stream.
3. Select the desired setting from the list.

NOTICE!

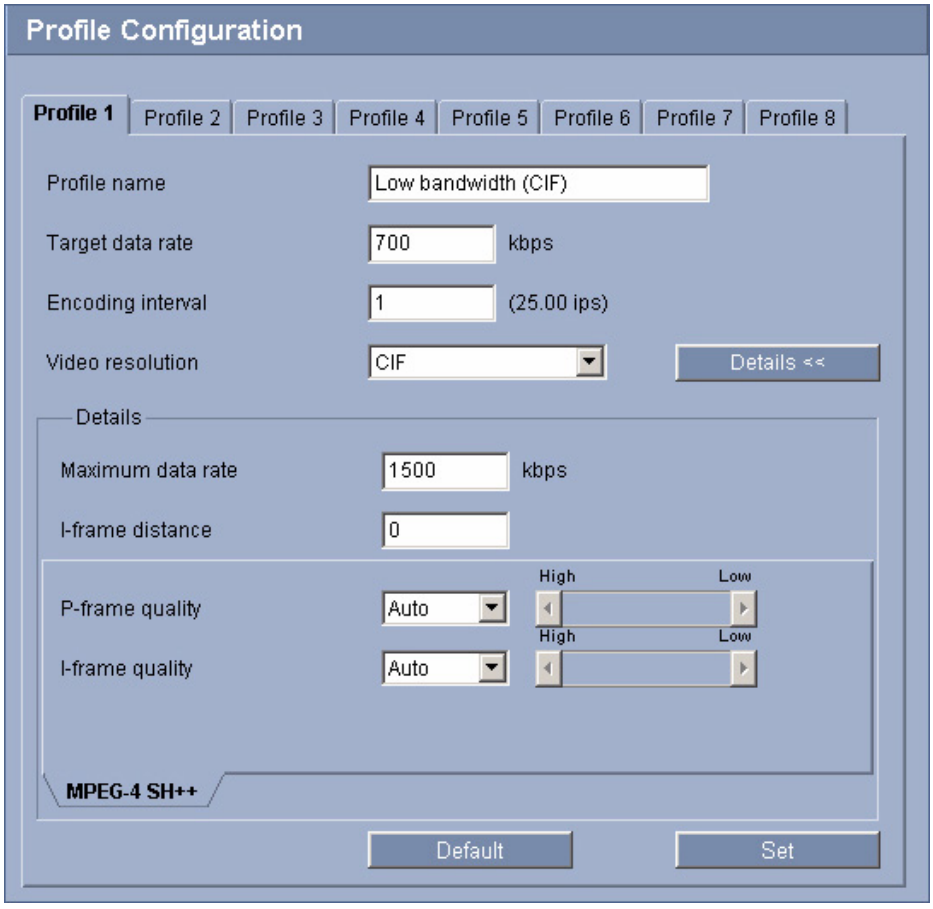
By default, Stream 2 is transmitted for alarm connections and automatic connections. Bear this fact in mind when assigning the profile.

5.11.2 Preview for

Select which video data stream should be displayed in the previews. You can deactivate the display of the video images if the performance of the computer is affected too strongly by the decoding of the data streams.

Check the box for the required data stream.

5.12 Profile Configuration



You can change individual parameter values within a profile and you can also change the name. You can switch between profiles by clicking the appropriate tabs.

CAUTION!
The profiles are rather complex. They include a large number of parameters that interact with one another, so it is generally best to use the default profiles.
Change the profiles only once you are fully familiar with all the configuration options.

NOTICE!
All parameters combine to make up a profile and are dependent on one another. If you enter a setting that is outside the permitted range for a particular parameter, the nearest permitted value will be substituted when the settings are saved.

5.12.1 Profile name

You can enter a new name for the profile here. The name is then displayed in the list of available profiles in the **Active profile** field.

5.12.2 Target data rate

You can limit the data rate for the VideoJet X20 to optimize utilization of the bandwidth in your network. The target data rate should be set according to the desired picture quality for typical scenes with no excessive motion.
For complex images or frequent changes of image content due to frequent movements, this limit can be temporarily exceeded up to the value you enter in the **Maximum data rate** field.

5.12.3 Encoding interval

The figure selected here determines the interval at which images are encoded and transmitted. For example, entering **4** means that only every fourth image is encoded, the following three are skipped — this can be particularly advantageous with low bandwidths. The image rate in ips (images per second) is displayed next to the text field.

5.12.4 Video resolution

Here you can select the desired resolution for the MPEG-4 video image. The following resolutions are available:

- **QCIF**
  176 × 144/120 pixels
- **CIF**
  352 × 288/240 pixels
- **1/2 D1**
  352 × 576/480 pixels
- **2CIF**
  704 × 288/240 pixels
- **4CIF/D1**
  704 × 576/480 pixels
- **2/3 D1**
  464 × 576/480 pixels

5.12.5 Default

Click **Default** to return the profile to the factory default values.

5.12.6 Details

Clicking the **Details >>** button displays further details on image quality and data transmission. These settings require extensive knowledge of the MPEG standard and video data compression. Incorrect settings can render the video images unusable.

5.12.7 Maximum data rate

This maximum data rate is not exceeded under any circumstances. Depending on the video quality settings for the I- and P-frames, this fact can result in individual images being skipped. The value entered here must be at least 10% higher than the value entered in the **Target data rate** field. If the value entered here is too low, it will automatically be adjusted.

5.12.8 I-frame distance

This parameter allows you to set the intervals in which the I-frames will be coded. **0** means auto mode, whereby the video server inserts I-frames as necessary. An entry of **1** indicates that I-frames are continuously generated. An entry of **2** indicates that only every second image is an I-frame, and **3** only every third image etc.; the frames in between are coded as P-frames.

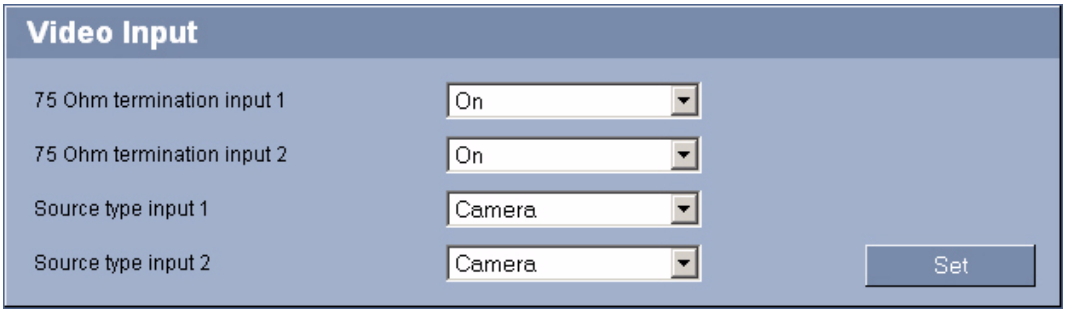
5.12.9 P-frame quality

This setting allows you to adjust the image quality of the P-frames depending on the movement within the image. The **Auto** option automatically adjusts to the optimum combination of movement and image definition (focus). Selecting **Manual** allows you to set a value between 4 and 31 on the slide control. The value **4** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **31** results in a very high refresh rate and lower image quality.

5.12.10 I-frame quality

This setting allows you to adjust the image quality of the I-frames. The **Auto** option automatically adjusts the quality to the settings for the P-frame video quality. Selecting **Manual** allows you to set a value between 4 and 31 on the slide control. The value **4** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **31** results in a very high refresh rate and lower image quality.

5.13 Video Input



You can activate the 75 Ohm terminating resistance for each video input on the VideoJet X20. The terminating resistance must be deactivated for the video signal to be looped through. Every video input is closed at the time of delivery.

NOTICE!
The numbering follows the labeling of the video inputs on the actual unit.

5.13.1 75 Ohm termination

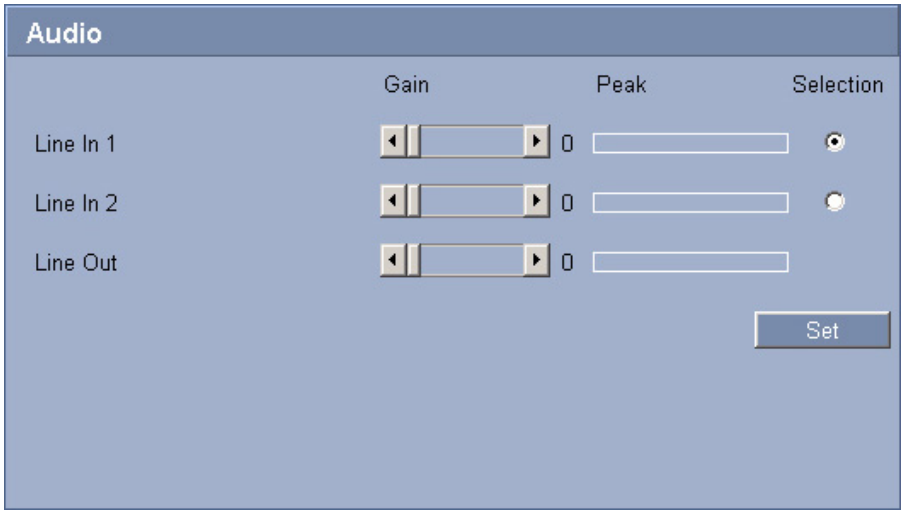
Select **Off** if the video signal is to be looped through.

5.13.2 Source type

To allow VCRs to be connected as a video source, you can change the characteristic of the video source from the preset value of **Camera** to **VCR**. VCRs require a more tolerant setting for the internal PLL as a result of jitter effects caused by the mechanical components of a VCR.

NOTICE!
In some cases, selecting the **VCR** option can lead to an improvement in the video image even with a camera connected.

5.14 Audio



You can set the gain of the audio signals to suit your specific requirements. The current video image is shown in the small window next to the slide controls to help you check the selected audio source and improve assignments. Your changes are effective immediately.
If you connect via Web browser you must activate the audio transmission on the **Livepage Configuration** page (see *Section 5.32 Livepage Configuration*, page 85). For other connections, the transmission depends on the audio settings of the respective system.

NOTICE!
The numbering of the audio inputs follows the labeling on the unit and the assignment to the respective video inputs. The assignment cannot be changed for Web browser connections.

5.14.1 Line In

You can set the audio signal gain for the line inputs. Make sure that the display does not go beyond the green zone during modulation.

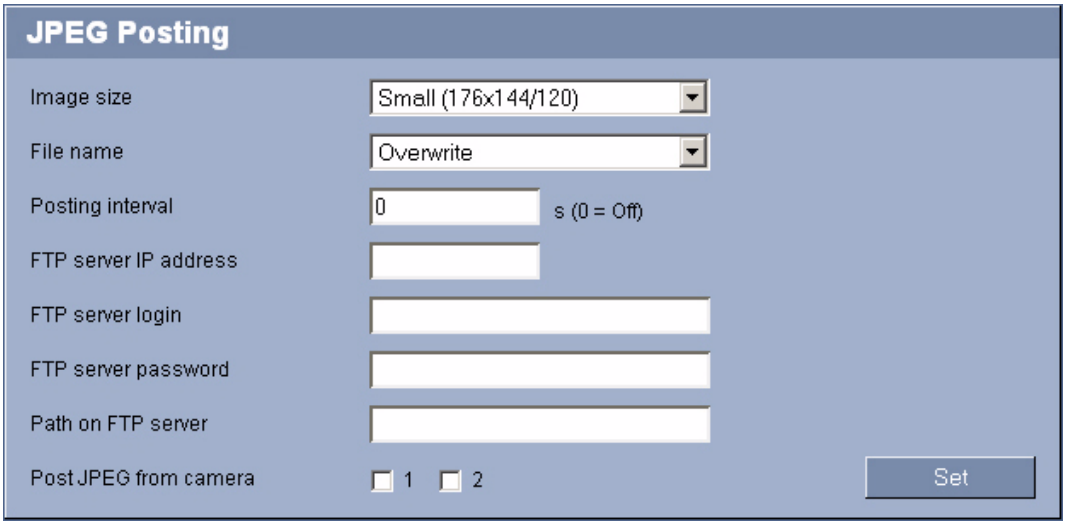
5.14.2 Line Out

You can set the line output gain. Make sure that the display does not go beyond the green zone during modulation.

5.14.3 Selection

Click one of the option boxes and then click **Set** to display the level of the respective audio input for orientation and to set the gain.

5.15 JPEG Posting



You can save individual JPEG images on an FTP server at specific intervals. You can then retrieve these images at a later date to reconstruct alarm events if required.

5.15.1 Image size

Select the resolution you wish the JPEG images to have:

- **Small**
  176 × 144/120 pixels (QCIF)
- **Medium**
  352 × 288/240 pixels (CIF)
- **Large**
  704 × 576/480 pixels (4CIF)

5.15.2 File name

You can select how file names will be created for the individual images that are transmitted.

- **Overwrite**
  The same file name is always used and any existing file will be overwritten with the current file.
- **Increment**
  A number from 000 to 255 is added to the file name and automatically incremented by 1. When it reaches 255 it starts again from 000.
- **Date/time suffix**
  The date and time are automatically added to the file name. When setting this parameter, ensure that the unit's date and time are always correctly set. Example: the file snap011005_114530.jpg was stored on October 1, 2005 at 11:45 and 30 seconds.

5.15.3 Posting interval

Enter the interval in seconds at which the images will be sent to an FTP server. Enter zero if you do not want any images to be sent.

5.15.4 FTP server IP address

Enter the IP address of the FTP server on which you wish to save the JPEG images.

5.15.5 FTP server login

Enter your login name for the FTP server.

5.15.6 FTP server password

Enter the password that gives you access to the FTP server.

5.15.7 Path on FTP server

Enter the exact path on which you wish to post the images on the FTP server.

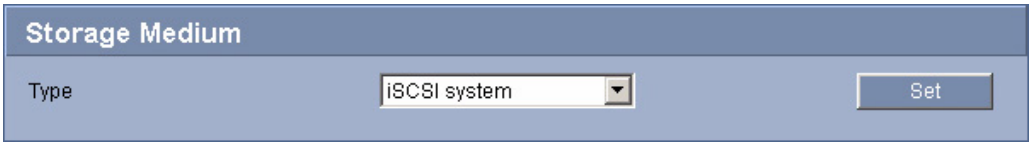
5.15.8 Post JPEG from camera

Click the checkbox to activate the camera input for the JPEG image. An enabled camera input is indicated by a check mark.

NOTICE!

The numbering follows the labeling of the video inputs on the actual unit.

5.16 Storage Medium



You can record the images from the cameras connected to the VideoJet X20 on various local storage media or on an appropriately configured iSCSI system.
The internal RAM memory of the VideoJet X20 is suitable for short-term recordings and pre-alarm recordings in ring mode operation.
CF cards (see *Section 4.3.6 CF Slot*, page 21) are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions.
If the VideoJet X20 has a hard drive, this is suitable for longer, local recordings in mobile use. For long-term, authoritative images in stationary operation, it is essential that you use an appropriately sized iSCSI system.
It is also possible to let the Video Recording Manager (**VRM**) control all recording when accessing an iSCSI system. The VRM is an external program for configuring recording tasks for video servers. For further information please contact your local customer service at Bosch Security Systems.

5.16.1 Type

Select the desired storage medium to subsequently configure the recording parameters.
If you select **VRM**, the Video Recording Manager will manage all recording, and you will not be able to make any further configurations here.

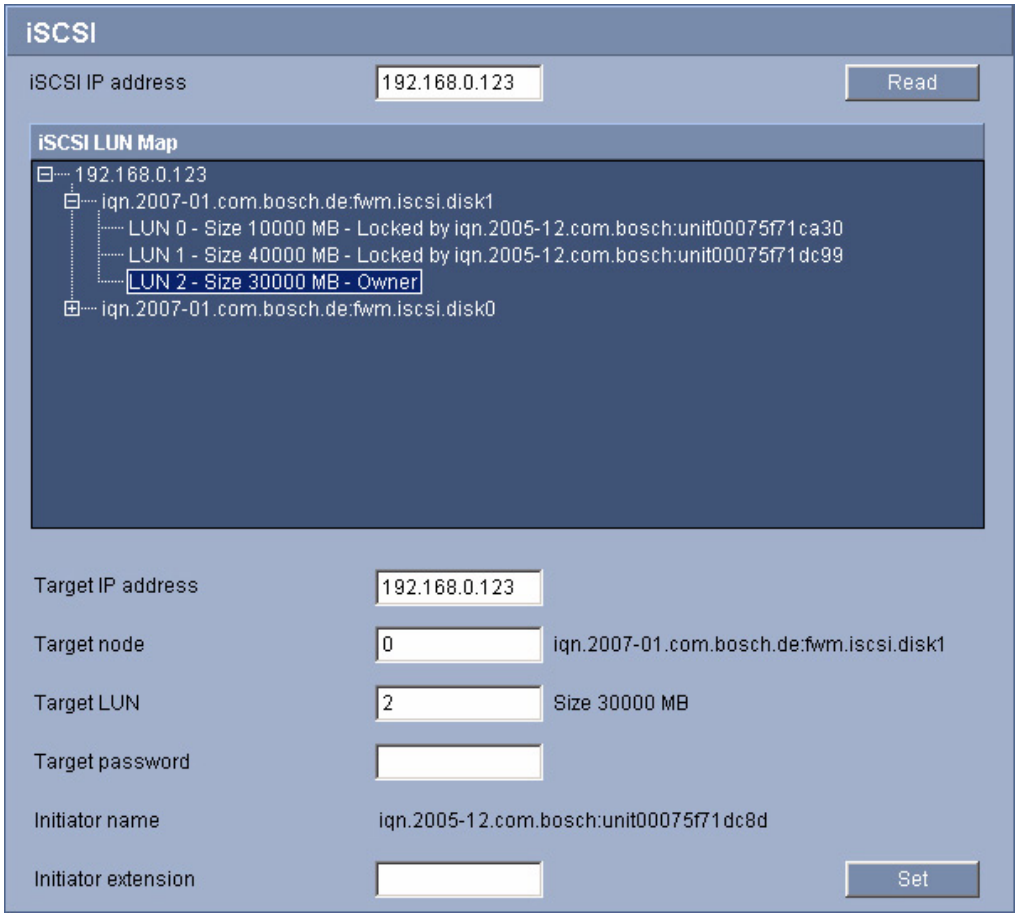
CAUTION!
If you switch the storage medium from **iSCSI system** to another option, the settings on the **iSCSI** page will be lost and can only be restored by reconfiguring them.

5.16.2 Storage Information

The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

1. Click **Log** to view a status report with logged actions. A new window will open.
2. In this window, click **Clear** to delete all entries. The entries will be deleted immediately. This action cannot be reversed.
3. Click the **Close** button to close the window.

5.17 iSCSI



If you select type **iSCSI system** as the storage medium, you then need to set up a connection to the desired iSCSI system and set the configuration parameters.

NOTICE!
The storage system selected must be available on the network and completely set up. Amongst other things, it must have an IP address and be divided into logical drives (LUN).

5.17.1 iSCSI IP address

1. Enter the IP address of the required iSCSI target here.
2. Click the **Read** button. The connection to the IP address will be established. The **iSCSI LUN Map** field contains the corresponding logical drives.

5.17.2 iSCSI LUN Map

The LUN map displays the logical drives configured for the iSCSI system. The current user is displayed for each drive.

1. Double-click a free drive (LUN). The associated information is called up and automatically displayed in the fields below the map.
2. If the logical drive is password protected, you must first enter the password in the **Target password** field and click the **Set** button.

In cases where the information cannot be read due to the network topology, you must enter the data manually, so that the VideoJet X20 can access the drive. In this case you should ensure that the entries correspond exactly with the configuration of the iSCSI system.

1. Enter the required data into the corresponding fields.
2. Click the **Set** button. The VideoJet X20 will now use this data to try and connect to the required drive.

As soon as a connection has been established, the selected drive is used for recordings.

5.17.3 Target IP address

Enter the IP address of the required iSCSI target here.

5.17.4 Target node

Enter the number of the iSCSI target node.

5.17.5 Target LUN

Enter the LUN of the required drive.

5.17.6 Target password

If the drive is password protected, enter the password.

NOTICE!

You may not enter a new password. This is only possible by configuring the iSCSI system.

5.17.7 Initiator name

The initiator name is automatically displayed after a connection has been established.

5.17.8 Initiator extension

Enter the initiator extension. For the sake of clarity, you can enter a name or the existing extension with a comment, for example "– Camera 2".

5.17.9 Decoupling the Drive in Use

Each drive can only be associated with one user. If a drive is already being used by another user, you can decouple the user and connect the drive with the VideoJet X20.

CAUTION!
Before decoupling, make absolutely sure that the previous user no longer needs the drive.

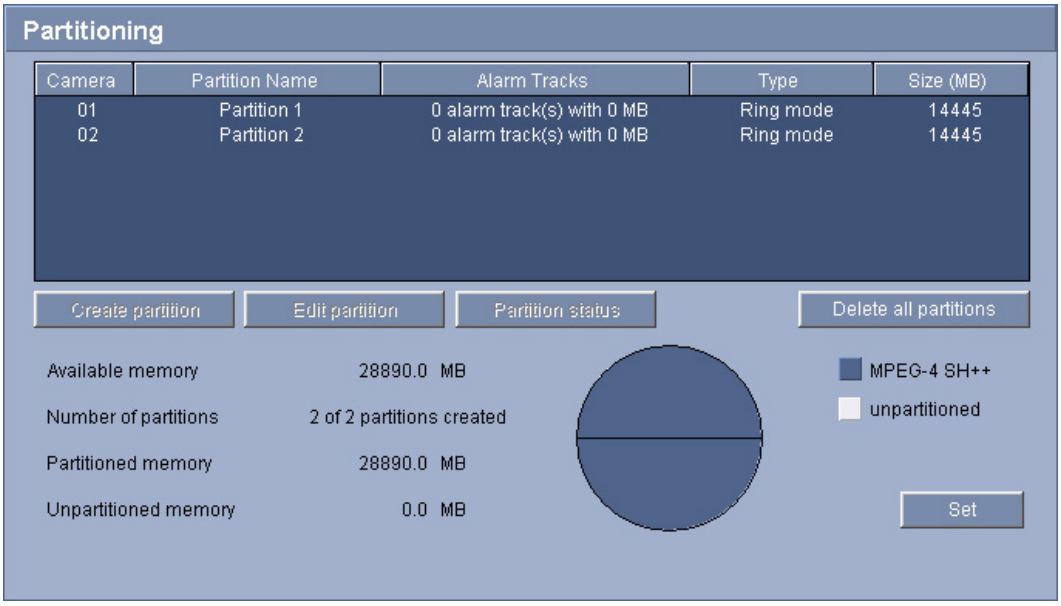
1. Double-click a drive that is already being used in the LUN map. You will see a warning message.
2. Confirm the decoupling of the current user. The drive is released and can now be connected to the VideoJet X20.

5.17.10 Storage Information

The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

1. Click **Log** to view a status report with logged actions. A new window will open.
2. In this window, click **Clear** to delete all entries. The entries will be deleted immediately. This action cannot be reversed.
3. Click the **Close** button to close the window.

5.18 Partitioning



Two partitions can be set up for recordings of the cameras connected to the VideoJet X20; this is similar to the partitioning often found on computer hard drives. Parameters such as size and type of video recording can be specified for each partition. Modifying these parameters leads to reorganization, during which stored data is lost.

The unit requires a dedicated partition for the recordings of each connected camera. Each partition is linked to its own encoder or camera input: camera input **Video In 1** with partition number **01**, camera input **Video In 2** with partition **02**. This assignment cannot be modified. As a result, all numbers are always displayed in the list, regardless of whether a corresponding partition is available or has been deleted. Both potential partitions need to be configured in order to record two cameras.

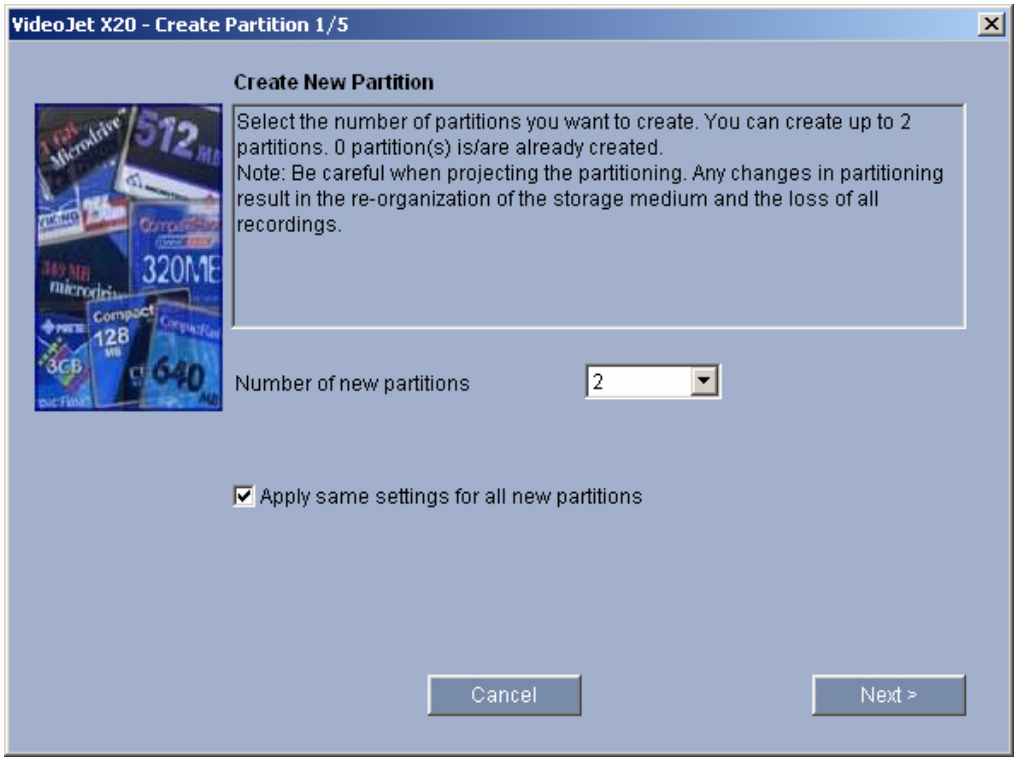
All partitions are listed in the table on the **Partitioning** page together with the number of the video input (**Camera**), their partition name, alarm tracks, type and size.
In addition, the page provides you with an overview of the drive data; for example total memory and number of partitions created. A pie chart indicates how much memory space is partitioned for recordings.

5.18.1 Creating a Partition

NOTICE!
The maximum number of partitions is predefined and corresponds to the number of video inputs on the unit.
You can create multiple partitions of the same type in one process. To do this, check the box **Apply same settings for all new partitions** in the first window.

Creating a new partition is performed using separate windows in which information is presented to you and you are led step by step through the necessary settings.
The process must be completed for each partition to be set up on the hard drive. After startup, you can select the total number of partitions to be set up. The setup process is then started as often as is necessary to configure all partitions.

1. Click the **Create partition** button to start the assistant for creating partitions. The first window appears.


VideoJet X20 - Create Partition 1/5
Create New Partition
Select the number of partitions you want to create. You can create up to 2 partitions. 0 partition(s) is/are already created.
Note: Be careful when projecting the partitioning. Any changes in partitioning result in the re-organization of the storage medium and the loss of all recordings.
Number of new partitions
2
Apply same settings for all new partitions
Cancel
Next >

2. You should always first read the information text in the upper section of the window.
3. Click in the text fields to enter values or use the other controls that are available, such as buttons, checkboxes or list fields.
4. Click the **Next >** button at the bottom of the window to continue with the next step.
5. Click the **< Back** button at the bottom of the window to view the previous step again.
6. Click the **Cancel** button to cancel the process and close the wizard.

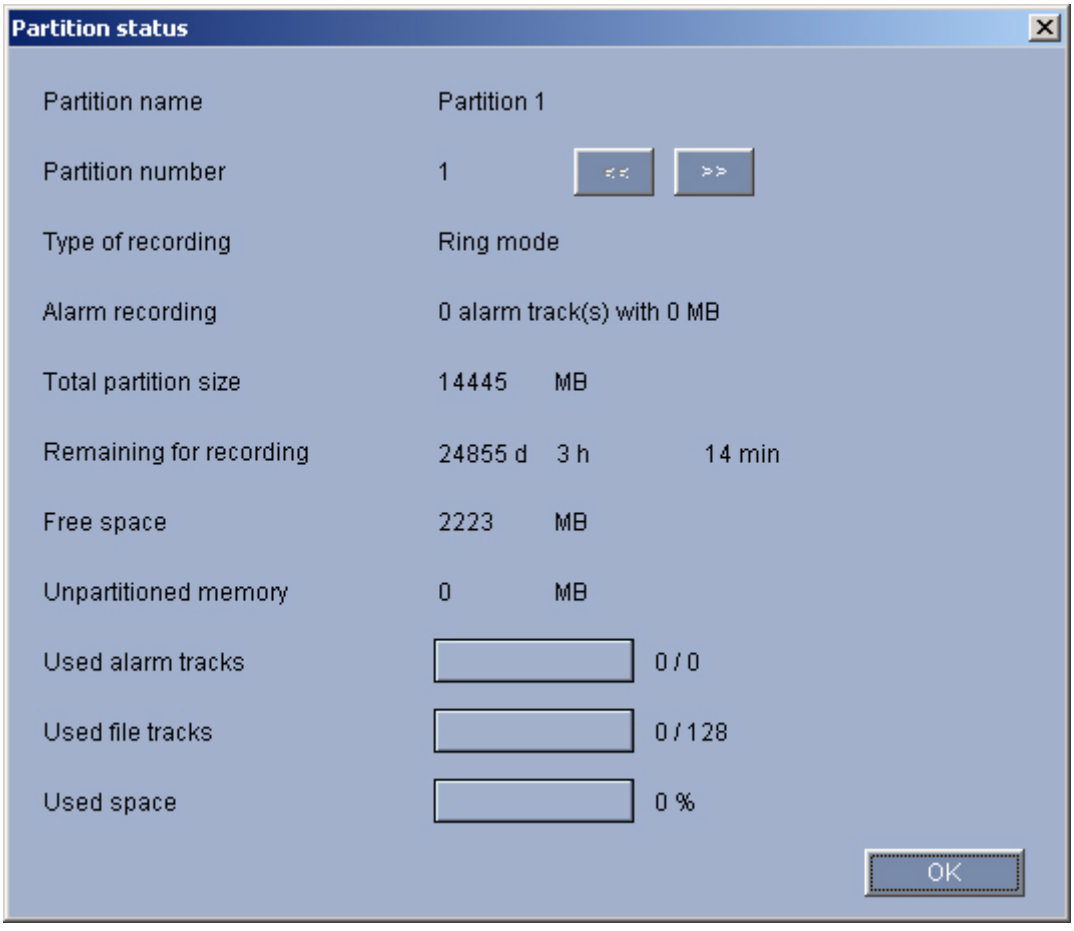
5.18.2 Saving Changes

After you have made all necessary settings, you must transfer the settings to the unit and save them.

CAUTION!
All modifications to settings are only effective if you complete the configuration in the last window by clicking **Finish**.

1. Switch to the last window.
2. Click **Finish** to complete the configuration. All settings are now transferred to the unit and subsequently become effective.

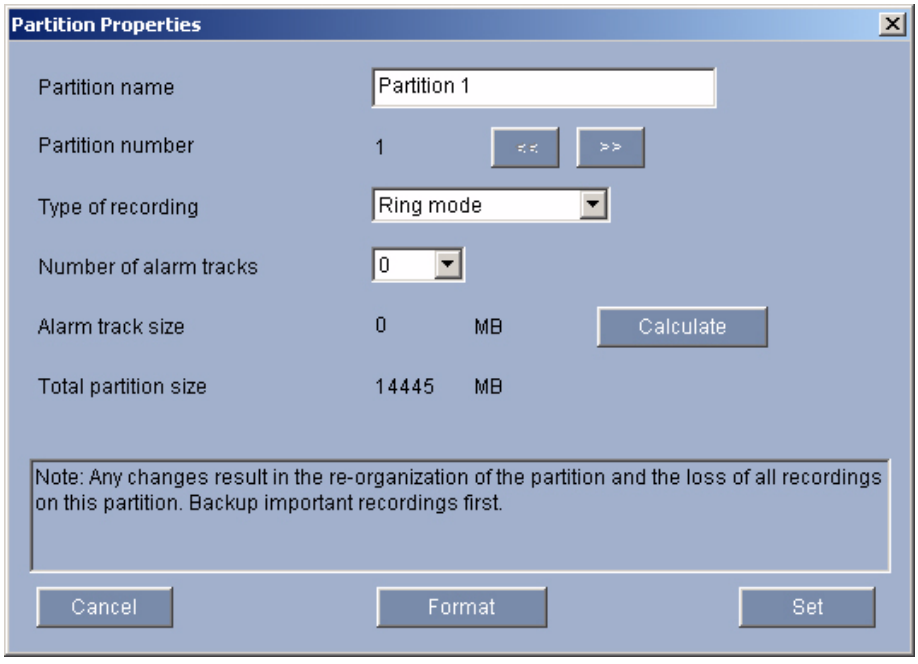
5.18.3 Partition status



The **Partition status** window provides you with an overview of the current partition configuration. No changes can be made here.

1. In the list, click the partition that you want to modify in order to select this partition.
2. Click the **Partition status** button. A new window with the entries for the selected partition is opened.
3. Click the **<<** and **>>** buttons to view the status of other partitions.
4. Click **OK** to close the window.

5.18.4 Editing a Partition



You can modify the configuration of a partition at any time.

CAUTION!
All modifications result in the reorganization of the partition and all sequences stored on it are therefore lost.
Consequently, you should back up all important sequences on the computer's hard drive before modifying the partition.

You can perform the required modifications in the **Partition Properties** window.

1. In the list, click the partition that you want to modify in order to select this partition.
2. Click the **Edit partition** button. A new window with the entries for the selected partition is opened.
3. Make the desired changes.
4. Click the **<<** and **>>** buttons to edit other partitions.
5. Click the **Set** button to save the modifications.

5.18.5 Partition name

You can enter a new name for the partition.

5.18.6 Partition number

The partition number (= number of the video input) is displayed for information purposes.

5.18.7 Type of recording

Select the required recording type.
In the case of **Ring mode** the recording proceeds continuously. If the maximum hard drive space has been reached, the oldest recordings are automatically overwritten.
In the case of **Linear mode** the recording proceeds until the entire hard drive space is full. The recording is then stopped until old recordings have been deleted.

5.18.8 Number of alarm tracks

CAUTION!
Alarm tracks must be set up in the required partition for alarm recording.

The unit uses a special recording mode during alarm recording for optimal usage of storage capacity: as soon as a time gap for alarm recording begins, a recording is continuously made on one segment, which is the size of a complete alarm sequence (pre- and post-alarm time). This segment in the partition functions in a similar manner to a ring buffer and is overwritten until an alarm is actually triggered. Recording occurs on the segment only for the duration of the preset post-alarm time and a new segment is subsequently used in the same manner.
Select the number of alarm tracks to be used in the partition. One alarm event can be recorded in each alarm track. Accordingly, the number of alarms entered can be recorded and archived. A partition can contain a maximum of 128 alarm recordings.
If the **Ring mode** option is set for the partition, the latest alarm recordings are always saved in the preset number. If the **Linear mode** option is selected for the partition, the recording is stopped as soon as the total number of alarm tracks has been recorded.

5.18.9 Alarm track size

The size for the alarm tracks can be calculated using various parameters. The calculated size applies for each of the alarm tracks.

1. Click the **Calculate** button. A new window will open.
2. Select the setting you require from individual parameter list fields.
3. Click the **Set** button to apply the calculated value.

5.18.10 Format

You can delete all recordings in a partition at any time.

CAUTION!
Check the recordings before deleting and back up important sequences on the computer's hard drive.

▶ Click the **Format** button to delete all recordings in the currently selected partition.

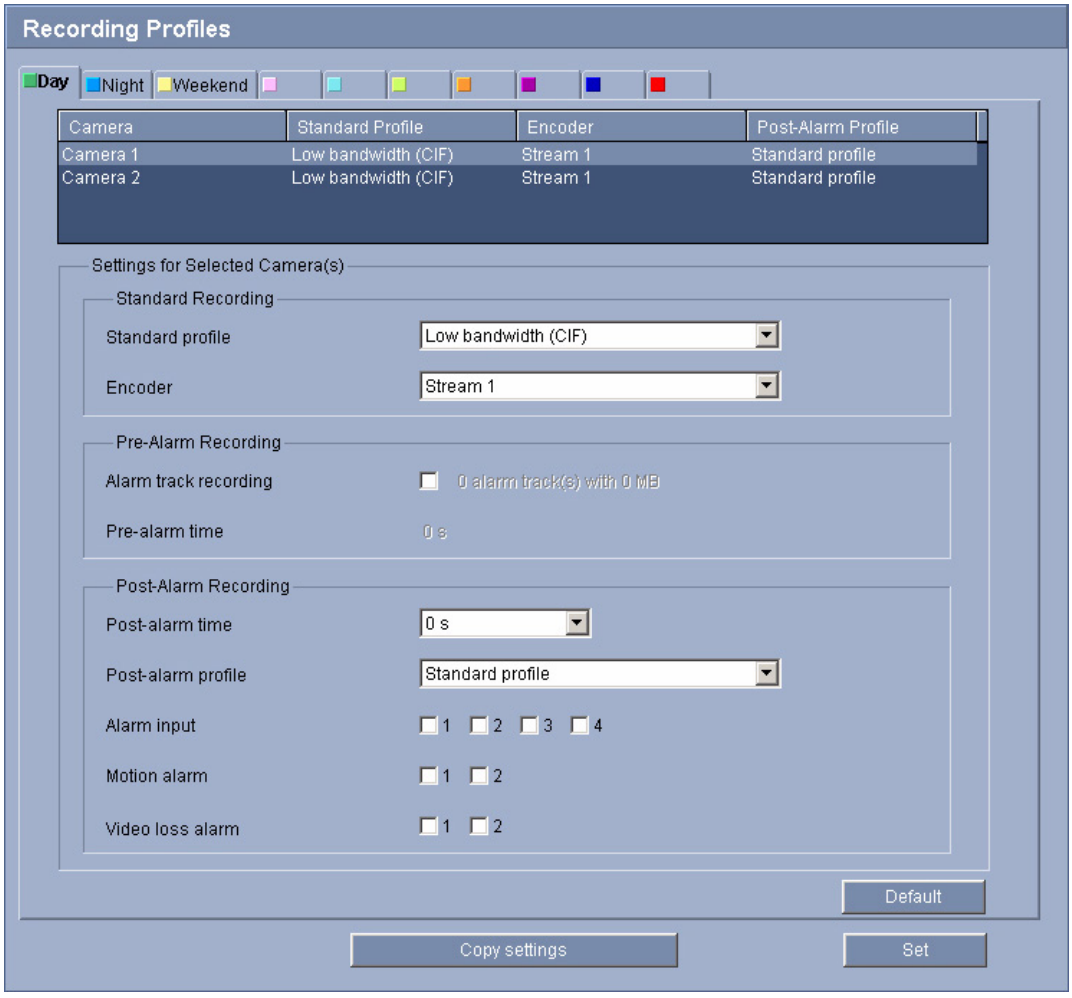
5.18.11 Deleting All Partitions

You can delete all partitions at any time. Individual partitions cannot be deleted.

CAUTION!
Deleting partitions causes reorganization of the entire hard drive and all sequences stored on it are therefore lost.
Consequently, you should check the recordings before deleting any partitions and back up important sequences on the computer's hard drive.

▶ Click the **Delete all partitions** button. The display retains the lines containing the numbers, the partition names are deleted and **0** is specified as the size in each case.

5.19 Recording Profiles



You can define up to ten different recording profiles. You will then use these recording profiles in the recording scheduler, where they are linked with the individual days and times (see *Section 5.20 Recording Scheduler*, page 58).
In each profile you can configure different settings for each camera input.

NOTICE!
You can change or add to the recording profile description on the tabs on the **Recording Scheduler** page (see *Section 5.20.3 Time Periods*, page 59).

1. Click one of the tabs to edit the corresponding profile.
2. In the table, click the name of the camera input for which you want to edit the settings.
3. You can select multiple camera inputs by holding down the shift or [Ctrl] key as usual in Windows. The following settings apply to all selected entries.
4. Click the **Default** button to return all settings to their default, if appropriate.
5. Click the **Copy settings** button if you want to copy the currently visible settings to other profiles. A new window will open and you can select the profiles in which you want to copy the settings.
6. For each profile, click the **Set** button to save the settings in the unit.

5.19.1 Standard profile

From this field, you can select the encoder profile to be used for continuous recording (see *Section 5.11 Encoder Profile*, page 38).

NOTICE!
The recording profile can deviate from the standard setting **Active profile** for the video input set and is only used during an active recording.

5.19.2 Encoder

Here you can select the data stream to be used for the recording.

5.19.3 Alarm track recording

NOTICE!
This parameter is active only if alarm tracks have been configured for the camera input concerned, i.e. the corresponding partition (see *Section 5.18.8 Number of alarm tracks*, page 55).

- ▶ Click the checkbox to activate alarm track recording. The pre-alarm time is automatically displayed for information.

5.19.4 Post-alarm time

You can select the required post-alarm time from the list field.

5.19.5 Post-alarm profile

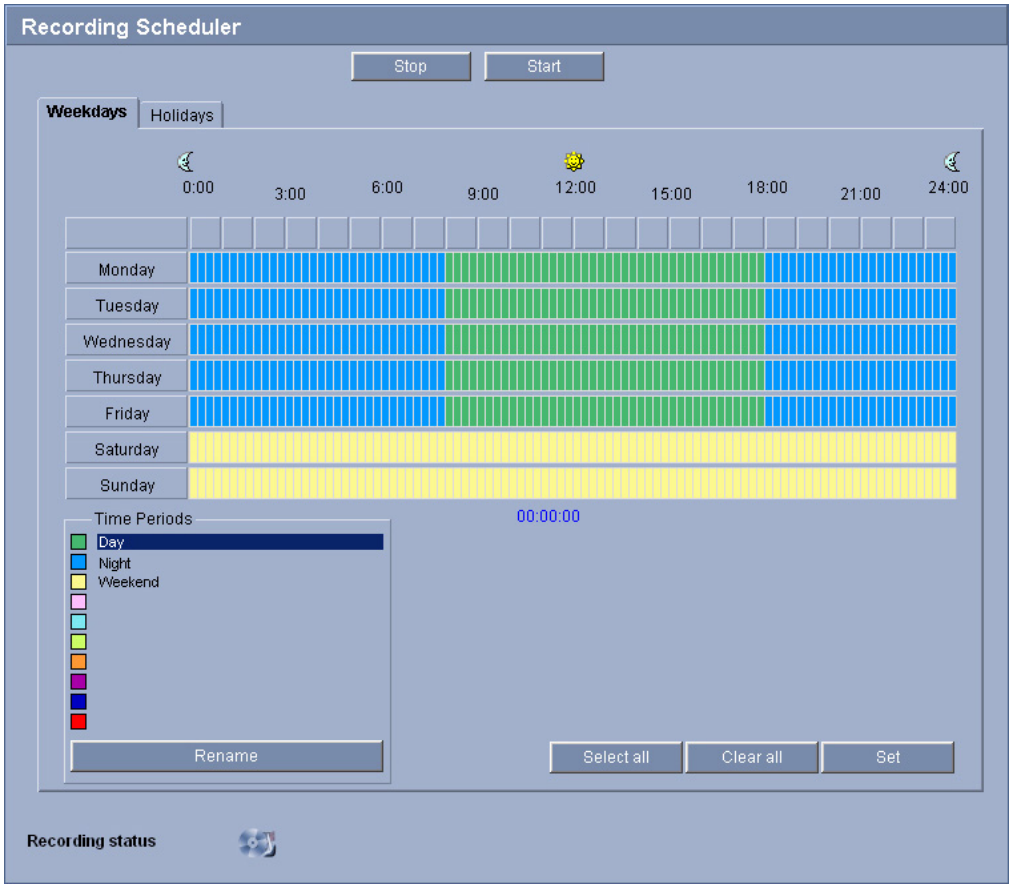
You can select the encoder profile to be used for recording during the post-alarm time (see *Section 5.11 Encoder Profile*, page 38).
The **Standard profile** option adopts the selection for continuous recordings at the top of the page.

5.19.6 Alarm input / Motion alarm / Video loss alarm

Here you can select the alarm sensor that is to trigger a recording. You can also use the motion and video alarm for a camera to trigger the alarm recording by another camera.

NOTICE!
The motion alarms are configured and activated for each camera on the **VCA** page (see *Section 5.23 VCA*, page 64).
The alarm inputs are configured and activated on the **Alarm Sources** page (see *Section 5.21 Alarm Sources*, page 60).
The numbering of the checkboxes for the alarm inputs corresponds to the labeling of the alarm inputs on the VideoJet X20. The motion and video alarm corresponds to the labeling on the video inputs.

5.20 Recording Scheduler



The recording scheduler allows you to link the created recording profiles with the days and times at which the images of selected cameras are to be recorded in the event of an alarm. You can link any number of 15 minute intervals with the recording profiles for each day of the week. Moving the mouse cursor over the table displays the time below it. This aids orientation.

In addition to the normal weekdays, you can define holidays that are not in the standard weekly schedule on which recordings are to apply. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

1. Click the profile you want to link in the **Time Periods** field.
2. Click in a field in the table, hold down the mouse button and drag the cursor over all the periods to be assigned to the selected profile.
3. Use the right mouse button to deselect any of the intervals.
4. Click the **Select all** button to link all time intervals to the selected profile.
5. Click the **Clear all** button to deselect all of the intervals.
6. When you are finished, click the **Set** button to save the settings in the unit.

5.20.1 Holidays

You can define holidays that are not in the standard weekly schedule on which recordings are to apply. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

1. Click the **Holidays** tab. Any days that have already been selected will be shown in the table.
2. Click the **Add** button. A new window will open.
3. Select the desired date from the calendar. You can select several consecutive calendar days by holding down the mouse button. These will later be displayed as a single entry in the table.
4. Click **OK** to accept the selection. The window will close.
5. Assign the individual holidays to the recording profiles, as described above.

5.20.2 Deleting Holidays

You can delete holidays you have defined yourself at any time.

1. Click the **Delete** button. A new window will open.
2. Click the date you wish to delete.
3. Click **OK**. The item will be deleted from the table and the window will close.
4. The process must be repeated for deleting additional days.

5.20.3 Time Periods

You can change the names of the recording profiles.

1. Click a profile and then the **Rename** button.
2. Enter your chosen name and then click the **Rename** button again.

5.20.4 Activating the Recording

After completing configuration you must activate the recording scheduler and start the recording. Once recording is underway, the **Recording Profiles** and **Recording Scheduler** pages are deactivated and the configuration cannot be modified.

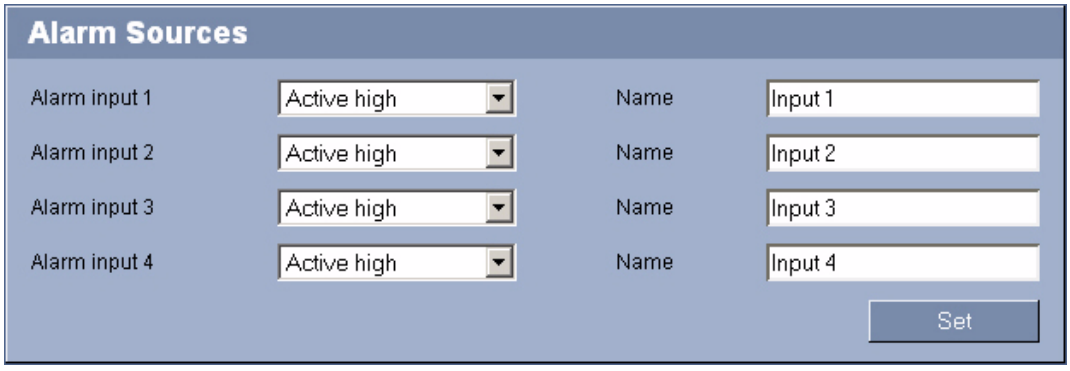
You can stop the recording activity at any time and modify the settings.

1. Click the **Start** button to activate the recording scheduler.
2. Click the **Stop** button to deactivate the recording scheduler. Recordings that are currently running will be interrupted and the configuration can be modified.

5.20.5 Recording status

The graphic indicates the recording activity of the VideoJet X20. You will see an animated graphic while recording is taking place.

5.21 Alarm Sources



You can configure the alarm inputs of the VideoJet X20.

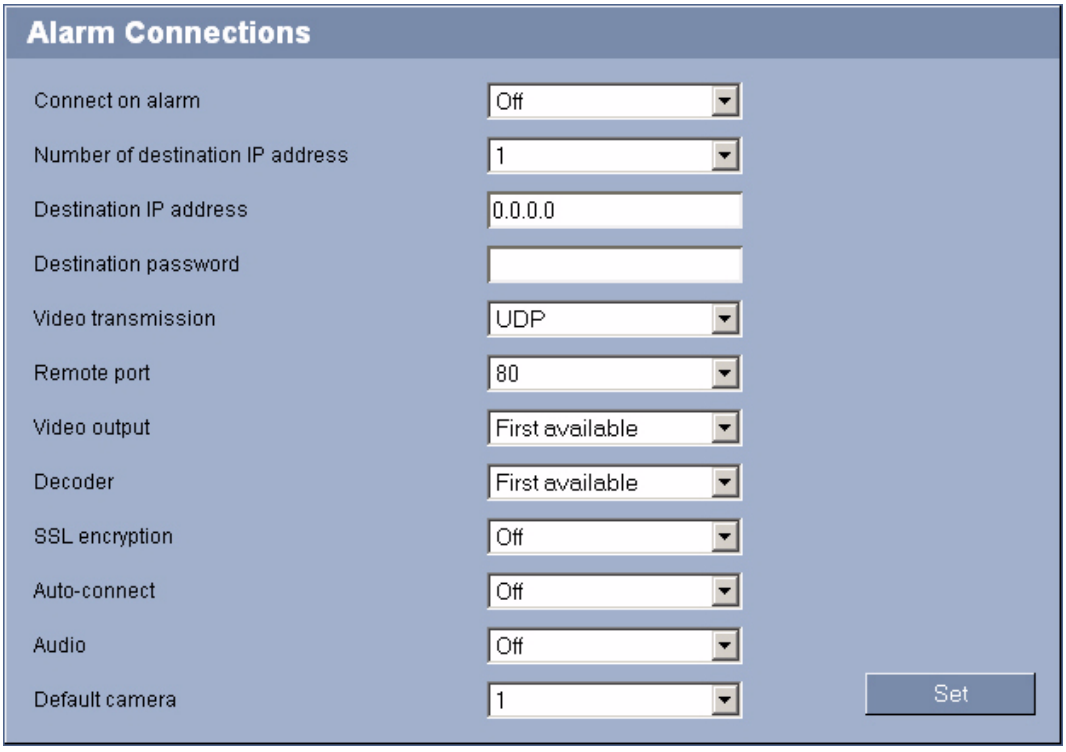
5.21.1 Alarm input

Select **Active high** if the alarm is to be triggered by closing the contact. Select **Active low** if the alarm is to be triggered by opening the contact.

5.21.2 Name

You can enter a name for each alarm input, which is then displayed below the icon for the alarm input on the **LIVEPAGE** if configured correctly (see *Section 5.32 Livepage Configuration*, page 85).

5.22 Alarm Connections



You can select how the VideoJet X20 responds to an alarm. In the event of an alarm, the unit can automatically connect to a pre-defined IP address. You can enter up to ten IP addresses which the VideoJet X20 will contact in order in the event of an alarm, until a connection is made.

5.22.1 Connect on alarm

Select **On** so that the VideoJet X20 automatically connects to a pre-defined IP address in the event of an alarm.

By setting **Follows input 1** the unit maintains the connection that has been automatically established for as long as an alarm exists on alarm input 1.

NOTICE!

By default, Stream 2 is transmitted for alarm connections. Bear this fact in mind when assigning the profile (see *Section 5.11 Encoder Profile*, page 38).

5.22.2 Number of destination IP address

Specify the numbers of the IP addresses to be contacted in the event of an alarm. The unit contacts the remote stations one after the other in the numbered sequence until a connection is made.

5.22.3 Destination IP address

For each number, enter the corresponding IP address for the desired remote station.

5.22.4 Destination password

If the remote station is password protected, enter the password here.
In this page, you can save a maximum of ten destination IP addresses and hence up to ten passwords for connecting to remote stations. If connections to more than ten remote stations are to be possible, for example when initiating connections via higher-ranking systems such as VIDOS or Bosch Video Management System, you can store a general password here. The VideoJet X20 can use this general password to connect to all remote stations protected with the same password. In this case, proceed as follows:

1. Select **10** from the **Number of destination IP address** list field.
2. Enter the address **0.0.0.0** in the **Destination IP address** field.
3. Enter your chosen password in the **Destination password** field.
4. Define this password as the **user** password for all remote stations to which a connection is to be possible.

NOTICE!
If you enter the destination IP address 0.0.0.0 for destination 10, the VideoJet X20 will no longer use this address for the tenth attempt at automatic connection in the event of an alarm. The parameter is then used only to save the general password.

5.22.5 Video transmission

If the unit is operated behind a firewall, **TCP (HTTP Port)** should be selected as the transfer protocol. For use in a local network, select **UDP**.

CAUTION!
Please note that in some circumstances, a larger bandwidth must be available on the network for additional video images in the event of an alarm, in case multicast operation is not possible. To enable multicast operation, select the **UDP** option for the **Video transmission** parameter here and on the **Network** page (see *Section 5.28.5 Video transmission*, page 77).

5.22.6 Remote port

Depending on the network configuration, select a browser port here. The ports for HTTPS connections will be available only if the **On** option is selected in the **SSL encryption** parameter.

5.22.7 Video output

If you know which unit is being used as the receiver, you can select the analog video output to which the signal should be switched. If the destination unit is unknown, it is advisable to select the **First available** option. In this case, the image is placed on the first free video output. This is an output on which there is no signal. The connected monitor only displays images when an alarm is triggered. If you select a particular video output and a split image is set for this output on the receiver, you can also select from **Decoder** the decoder in the receiver that is to be used to display the alarm image.

NOTICE!
Refer to the destination unit documentation concerning image display options and available video outputs.

5.22.8 Decoder

Select a decoder of the receiver to display the alarm image. The decoder selected has an impact on the position of the image in a split screen. For example, you can specify via a VIP XD that the upper-right quadrant should be used to display the alarm image by selecting decoder 2.

5.22.9 SSL encryption

The data for the connection, for example the password, can be securely transmitted with SSL encryption. If you have selected the **On** option, only encrypted ports are offered in the **Remote port** parameter.

NOTICE!
Please note that the SSL encryption must be activated and configured at both ends of a connection. This requires the appropriate certificates to be uploaded onto the VideoJet X20 (see *Section 5.35.4 Maintenance log*, page 90).

You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.30 Encryption*, page 82).

5.22.10 Auto-connect

Select the **On** option to automatically re-establish a connection to one of the previously specified IP addresses after each reboot, after a connection breakdown or after a network failure.

NOTICE!
By default, Stream 2 is transmitted for automatic connections. Bear this fact in mind when assigning the profile (see *Section 5.11 Encoder Profile*, page 38).

5.22.11 Audio

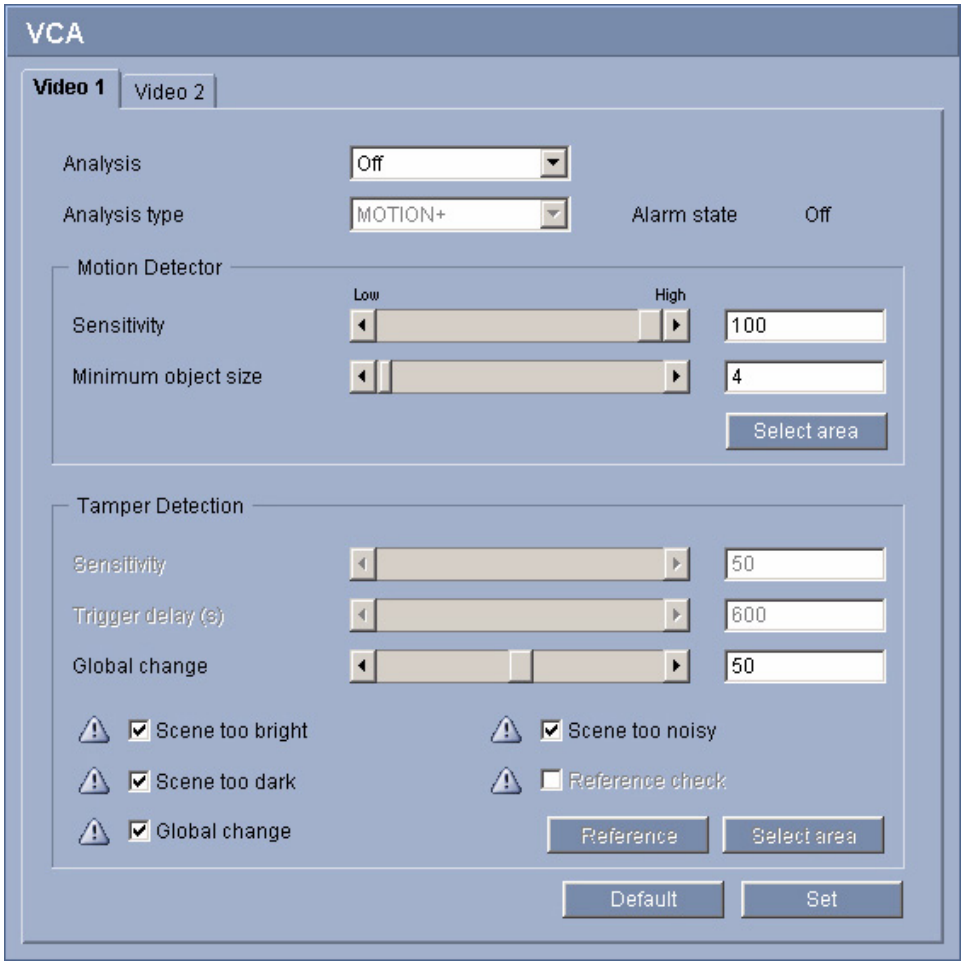
Select the **On** option if you wish to additionally transmit a standalone G.711-encoded audio stream with alarm connections.

5.22.12 Default camera

Here you can select the camera whose image will be automatically displayed first on the receiver when the alarm connection is made. Depending on the system configuration, the receiver can then select the other cameras as well.

NOTICE!
The numbering follows the labeling of the video inputs on the actual unit.

5.23 VCA



The VideoJet X20 features an integrated video content analysis (VCA), which can detect and analyze changes in the signal. Such changes can be due to movements in the camera's field of view.

NOTICE!
If computing power becomes short, the highest priority is always the live images and recordings. This can lead to impairment of the video content analysis. You should therefore observe the processor load and optimize the encoder settings or the video content analysis settings as necessary (see *Section 8.5 Processor Load*, page 115).

You can configure the video content analysis for each video input individually.

1. Click one of the tabs to open the configuration of the corresponding video input.
2. Enter the desired settings.
3. Click the **Default** button to return all settings to their default, if appropriate.

5.23.1 Analysis

Select the option **On** to activate the video content analysis.
As soon as the video content analysis is activated, metadata are created. Depending on the analysis type selected and the relevant configuration, additional information overlays the video image in the preview window next to the parameter settings. With the **MOTION+** analysis type, for example, the sensor fields in which motion is recorded will be marked with rectangles.

NOTICE!
On the **Livepage Configuration** page, you can also enable additional information overlays for the **LIVEPAGE** (see *Section 5.32 Livepage Configuration*, page 85).

5.23.2 Analysis type

Select the required analysis algorithm. By default, only **MOTION+** is available – this offers a motion detector and essential recognition of tampering. The current alarm status is displayed for information purposes.

NOTICE!
Additional analysis algorithms with comprehensive functions such as IVMD and IVA are available from Bosch Security Systems.
If you select one of these algorithms, you can set the corresponding parameters here directly. You can find information on this in the relevant documents on the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).

5.23.3 Motion Detector (MOTION+ only)

For the detector to function, the following conditions must be met:
- Analysis must be activated.
- At least one sensor field must be activated.
- The individual parameters must be configured to suit the operating environment and the desired responses.
- The sensitivity must be set to a value greater than zero.

CAUTION!
Reflections of light (off glass surfaces, etc.), switching lights on or off or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.
For indoor surveillance, ensure constant lighting of the areas during the day and at night.

5.23.4 Sensitivity (MOTION+ only)

The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject.
The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

5.23.5 Minimum object size (MOTION+ only)

You can specify the number of sensor fields that a moving object must cover to generate an alarm. This is to prevent objects that are too small from triggering an alarm.
A minimum value of **4** is recommended. This value corresponds to four sensor fields.

5.23.6 Select area (MOTION+ only)

The areas of the image to be monitored by the motion detector can be selected. The video image is subdivided into 858 square fields. Each of these fields can be activated or deactivated individually. If you wish to exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, etc.), the relevant fields can be deactivated.

1. Click **Select area** to configure the sensor fields. A new window will open.
2. If necessary, click **Clear all** first to clear the current selection (fields marked yellow).
3. Left-click the fields to be activated. Activated fields are marked yellow.
4. If necessary, click **Select all** to select the entire video frame for monitoring.
5. Right-click any fields you wish to deactivate.
6. Click **OK** to save the configuration.
7. Click the close button **X** in the window title bar to close the window without saving the changes.

5.23.7 Tamper Detection

You can reveal the tampering of cameras and video cables by means of various options. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

NOTICE!
The options for tamper detection can only be set for fixed cameras. Dome cameras or other motorized cameras cannot be protected in this manner as the movement of the camera itself causes changes in the video image that are too great.

5.23.8 Sensitivity

NOTICE!
This and the following parameter are only accessible if the reference check is activated.

The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject.
The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected.

5.23.9 Trigger delay (s)

You can set delayed alarm triggering. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This allows you to avoid false alarms triggered by short-term changes, for example cleaning activities in the direct field of vision of the camera.

5.23.10 Global change

You can set how large the global change in the video image must be for an alarm to be triggered. This setting is independent of the sensor fields selected under **Select area**. Set a high value if fewer sensor fields need to change to trigger an alarm. With a low value, it is necessary for changes to occur simultaneously in a large number of sensor fields to trigger an alarm.
This option allows you to detect, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mount bracket, for instance.

5.23.11 Scene too bright

Activate this function if tampering associated with exposure to extreme light (for instance, shining a flashlight directly on the lens) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

5.23.12 Scene too dark

Activate this function if tampering associated with covering the lens (for instance, by spraying paint on it) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

5.23.13 Scene too noisy

Activate this function if tampering associated with EMC interference (noisy scene as the result of a strong interference signal in the vicinity of the video lines), as an example, should trigger an alarm.

5.23.14 Global change

Activate this function if the global change, as set with the **Global change** slide control, should trigger an alarm.

5.23.15 Reference check

You can save a reference image that is continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This allows you to detect tampering that would otherwise not be detected, for example if the camera is turned.

1. Click **Reference** to save the currently visible video image as a reference.
2. Click **Select area** and select the areas in the reference image that are to be monitored.
3. Check the **Reference check** box to activate on-going matching. The stored reference image is displayed in black and white below the current video image, and the selected areas are marked in yellow.

5.23.16 Select area

You can select the image areas in the reference image that are to be monitored. The video image is subdivided into 858 square fields. Each of these fields can be activated or deactivated individually.

NOTICE!
Select only those areas for reference monitoring in which no movement takes place and that are always evenly lit, as false alarms could otherwise be triggered.

1. Click **Select area** to configure the sensor fields. A new window will open.
2. If necessary, click **Clear all** first to clear the current selection (fields marked yellow).
3. Left-click the fields to be activated. Activated fields are marked yellow.
4. If necessary, click **Select all** to select the entire video frame for monitoring.
5. Right-click any fields you wish to deactivate.
6. Click **OK** to save the configuration.
7. Click the close button **X** in the window title bar to close the window without saving the changes.

5.24 Alarm E-Mail

As an alternative to automatic connecting, alarm states can also be documented by e-mail. In this way it is possible to notify a recipient who does not have a video receiver. In this case the VideoJet X20 automatically sends an e-mail to a previously defined e-mail address.

5.24.1 Send alarm e-mail

Select **On** if you want the unit to automatically send an alarm e-mail in the event of an alarm.

5.24.2 Mail server IP address

Enter the IP address of a mail server that operates on the SMTP standard (Simple Mail Transfer Protocol). Outgoing e-mails are sent to the mail server via the address you entered. Otherwise leave the box blank (**0.0.0.0**).

5.24.3 SMTP user name

Enter a registered user name for the chosen mailserver here.

5.24.4 SMTP password

Enter the required password for the registered user name here.

5.24.5 Layout

You can select the data format of the alarm message.

- **Standard (with JPEG)**
  E-mail with attached JPEG image file.
- **SMS**
  E-mail in SMS format to an e-mail-to-SMS gateway (for example to send an alarm by cellphone) without an image attachment.

CAUTION!
When a cellphone is used as the receiver, make sure to activate the e-mail or SMS function, depending on the format, so that these messages can be received.
You can obtain information on operating your cellphone from your cellphone provider.

5.24.6 Attach JPEG from camera

Click the checkbox to specify the cameras from which JPEG images are sent. An enabled video input is indicated by a check mark.

5.24.7 Destination address

Enter the e-mail address for alarm e-mails here. The maximum address length is 49 characters.

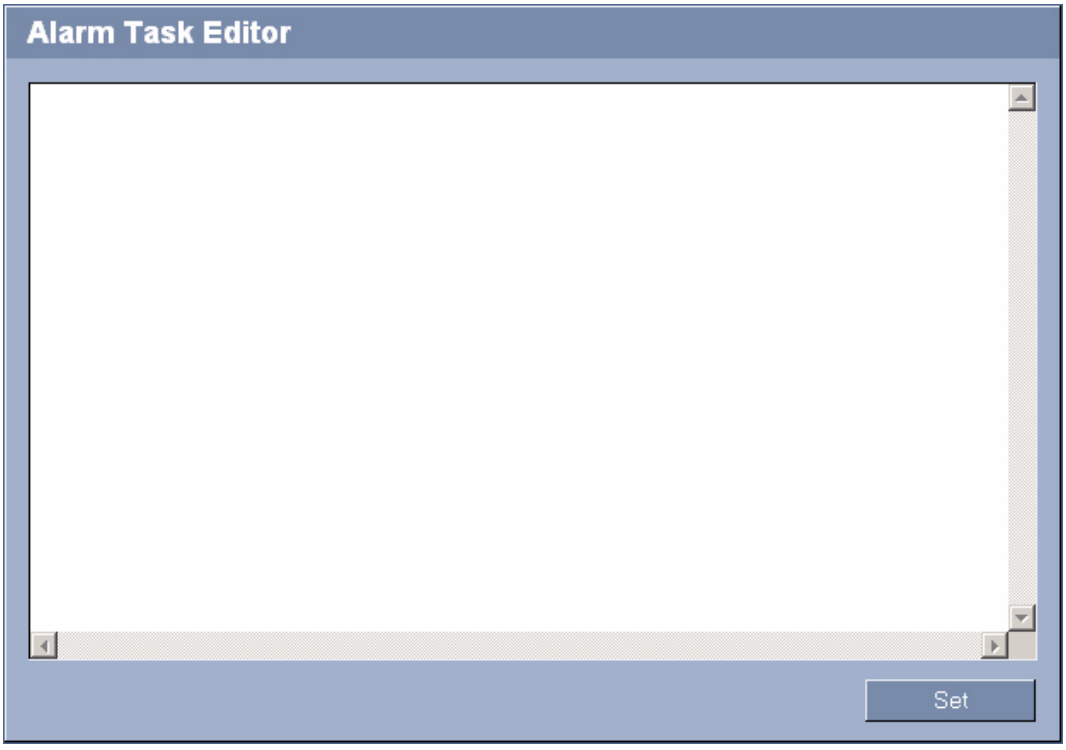
5.24.8 Sender name

Enter a unique name for the e-mail sender, for example the location of the unit. This will make it easier to identify the origin of the e-mail.

5.24.9 Test e-mail

You can test the e-mail function by clicking the **Send now** button. An alarm e-mail is immediately created and sent.

5.25 Alarm Task Editor



CAUTION!

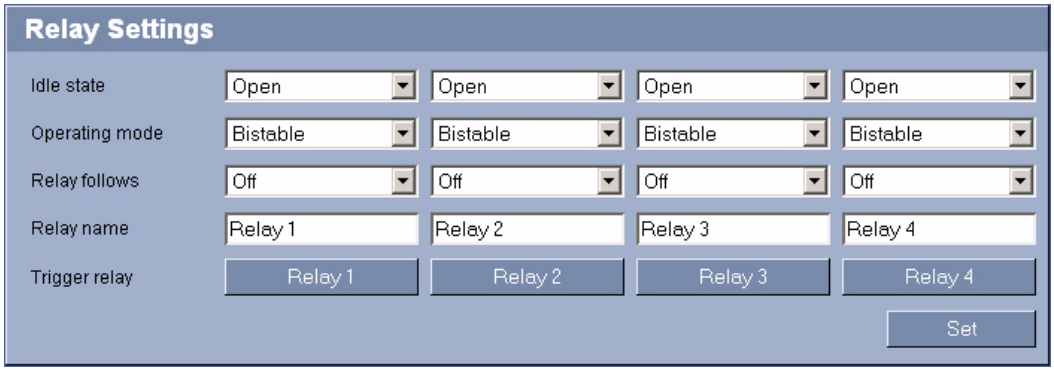
Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.

In order to edit this page, you must have programming knowledge and be familiar with the information in the **Alarm Task Script Language** document. You can find the document on the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).

As an alternative to the alarm settings on the various alarm pages, you can enter your desired alarm functions in script form here. This will overwrite all settings and entries on the other alarm pages.

1. Click the **Examples** link under the **Alarm Task Editor** field to see some script examples. A new window will open.
2. Enter new scripts in the **Alarm Task Editor** field or change existing scripts in line with your requirements.
3. When you are finished, click the **Set** button to transmit the scripts to the unit. If the transfer was successful, the message **Script successfully parsed** is displayed over the text field. If it was not successful, an error message will be displayed with further information.

5.26 Relay Settings



You can configure the switching behavior of the relay outputs. For each relay, you can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).
You can also specify whether an output should operate as a bistable or monostable relay. In bistable mode, the triggered state of the relay is maintained. In monostable mode, you can set the time after which the relay will return to the idle state.
You can select different events that automatically activate an output. It is possible, for example, to turn on a floodlight by triggering a motion alarm and then turning the light off again when the alarm has stopped.

5.26.1 Idle state

Select **Open** if you want the relay to operate as an NO contact, or select **Closed** if the relay is to operate as an NC contact.

5.26.2 Operating mode

Select an operating mode for the relay.
For example, if you want an alarm-activated lamp to stay on after the alarm ends, select **Bistable**. If you wish an alarm-activated siren to sound for ten seconds, for example, select **10 s**.

5.26.3 Relay follows

If required, select a specific event that will trigger the relay. The following events are possible triggers:

- **Off**
  Relay is not triggered by events
- **Connection**
  Trigger whenever a connection is made
- **Video alarm**
  Trigger by interruption of the video signal at the corresponding input
- **Motion alarm**
  Trigger by motion alarm at the corresponding input, as configured on the **VCA** page (see *Section 5.23 VCA*, page 64)
- **Local input**
  Trigger by the corresponding external alarm input
- **Remote input**
  Trigger by remote station's corresponding switching contact (only if a connection exists)

NOTICE!
The numbers in the lists of selectable events relate to the corresponding connections on the unit, **Video alarm 1**, for example to the **Video In 1** connection.

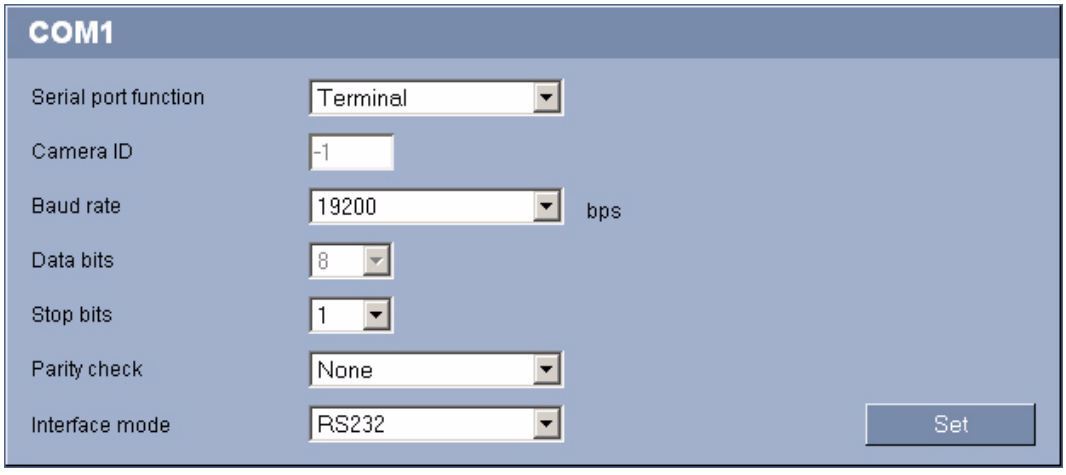
5.26.4 Relay name

You can assign a name for the relay here. The name is shown on the button next to **Trigger relay**. The Livepage can also be configured to display the name under the relay icon.

5.26.5 Trigger relay

Click the button to trigger the relay manually (for testing or to operate a door opener, for example).

5.27 COM1



You can configure the serial interface parameters (orange terminal block) to meet your requirements.

NOTICE!
If the VideoJet X20 is working in multicast mode (see *Section 5.29 Multicasting*, page 80), the first remote location to establish a video connection to the unit is also assigned the transparent data connection. However, after about 15 seconds of inactivity the data connection is automatically terminated and another remote location can exchange transparent data with the unit.

5.27.1 Serial port function

Select a controllable unit from the list. If you wish to use the serial port to transmit transparent data, select **Transparent**. Select **Terminal** if you wish to operate the unit from a terminal.

NOTICE!
After selecting a unit, the remaining parameters in the window are set automatically and should not be changed.

5.27.2 Camera ID

If necessary, enter the ID of the peripheral you wish to control (for example a dome camera or pan/tilt head). The entered ID relates to the peripheral that is connected to the first video input. For the second video input, the ID is automatically counted up and assigned to the peripheral connected to it.

5.27.3 Baud rate

Select the value for the transmission rate in bps.

5.27.4 Data bits

The number of data bits per character cannot be changed.

5.27.5 Stop bits

Select the number of stop bits per character.

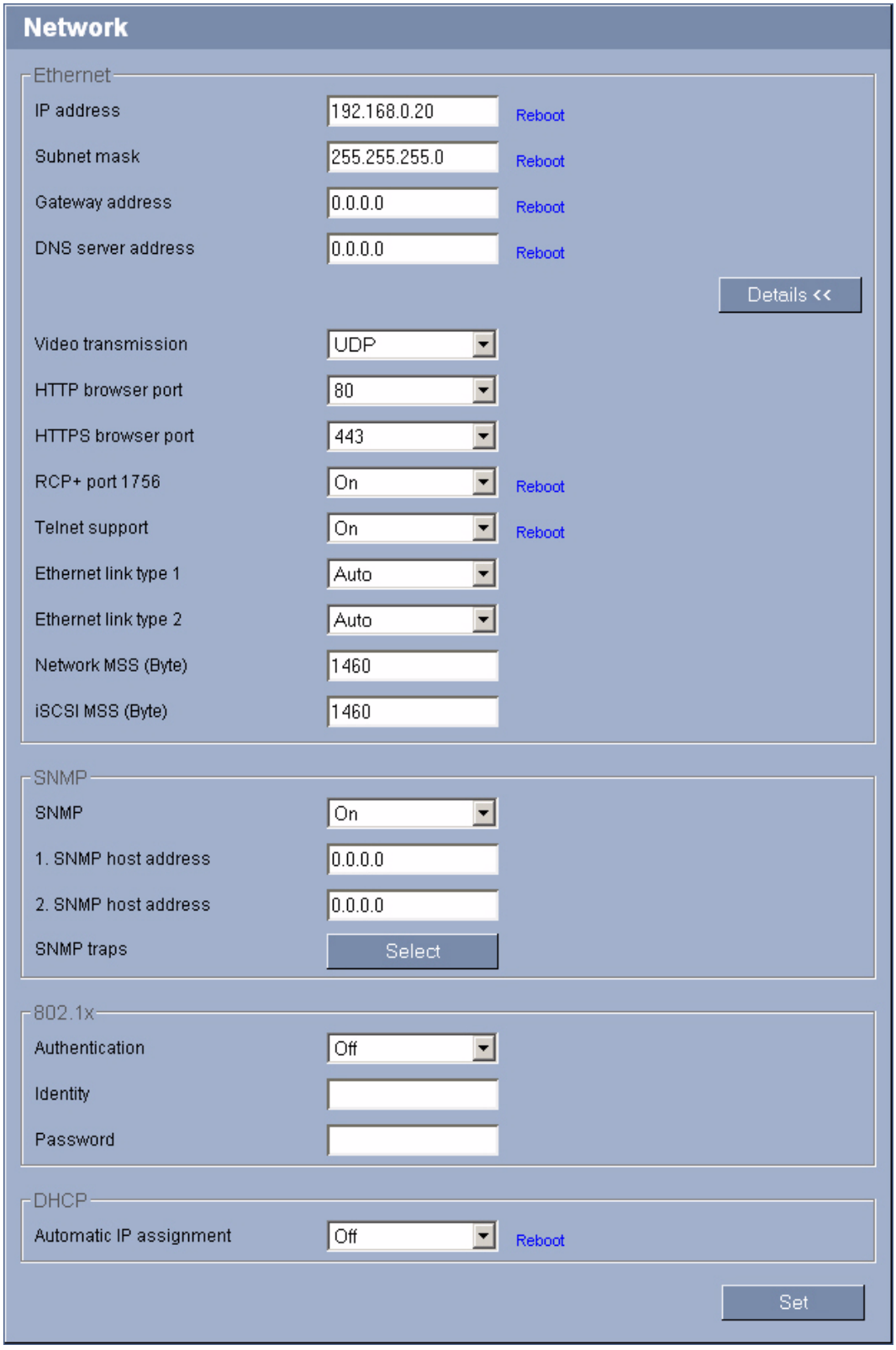
5.27.6 Parity check

Select the type of parity check.

5.27.7 Interface mode

Select the required protocol for the serial interface.

5.28 Network



The settings in this screen are used to integrate the VideoJet X20 into an existing network. Changes to fields followed by the **Reboot** link are transmitted to the unit by clicking the **Set** button; however, they will only be activated once the unit is rebooted.

1. Make the desired changes.
2. Click the **Set** button.
3. Click a **Reboot** link to trigger a reboot. VideoJet X20 is rebooted and the changed settings are activated.

CAUTION!
If you change the IP address, subnet mask or gateway address, the VideoJet X20 is only available under the new addresses after the reboot.

5.28.1 IP address

Enter the desired IP address for the VideoJet X20. The IP address must be valid for the network.

5.28.2 Subnet mask

Enter the appropriate subnet mask for the selected IP address here.

5.28.3 Gateway address

If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise leave the box blank (**0.0.0.0**).

5.28.4 DNS server address

The VideoJet X20 is easier to access if the unit is listed on a DNS server. If you wish, for example, to establish an Internet connection to the VideoJet X20, it is sufficient to enter the name given to the unit on the DNS server as a URL in the browser. Enter the DNS server's IP address. Servers are supported for secure and dynamic DNS.

5.28.5 Video transmission

If the unit is operated behind a firewall, **TCP (HTTP Port)** should be selected as the transfer protocol. For use in a local network, select **UDP**.

CAUTION!
Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.
The MTU value in UDP mode is 1,514 bytes.

5.28.6 HTTP browser port

Select a different HTTP browser port from the list if required. The default HTTP port is 80. If you want to allow only secure connections via HTTPS, you must deactivate the HTTP port. In this case, select **Off**.

5.28.7 HTTPS browser port

If you wish to allow browser access on the network via a secure connection, select an HTTPS browser port from the list if necessary. The default HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports; only unsecured connections will now be possible.
The VideoJet X20 uses the TLS 1.0 encryption protocol.You may have to activate this protocol via your browser configuration. You must also activate the protocol for the Java applications (via the Java control panel in the Windows control panel).

NOTICE!
If you want to allow only secure connections with SSL encryption, you must select the **Off** option for each of the parameters **HTTP browser port**, **RCP+ port 1756** and **Telnet support**. This deactivates all unsecured connections. Connections will then only be possible via the HTTPS port.

You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.30 Encryption*, page 82).

5.28.8 RCP+ port 1756

To exchange connection data, you can activate the unsecured RCP+ port 1756. If you want connection data to be transmitted only when encrypted, select the **Off** option to deactivate the port.

5.28.9 Telnet support

If you want to allow only secure connections with encrypted data transmission, you must select the **Off** option to deactivate Telnet support. The unit will then no longer be accessible using the Telnet protocol.

5.28.10 Ethernet link type 1

If necessary, select the Ethernet link type for interface **ETH 1**. Depending on the unit connected, it may be necessary to select a special operation type.

5.28.11 Ethernet link type 2

If necessary, select the Ethernet link type for interface **ETH 2**. Depending on the unit connected, it may be necessary to select a special operation type.

5.28.12 Network MSS (Byte)

You can set the maximum segment size for the IP packet's user data. This gives you the option to adjust the size of the data packets to the network environment and to optimize data transmission. Please comply with the MTU value of 1,514 bytes in UDP mode.

5.28.13 iSCSI MSS (Byte)

You can specify a higher MSS value for a connection to the iSCSI system than for the other data traffic via the network. The potential value depends on the network structure. A higher value is only useful if the iSCSI system is located in the same subnet as the VideoJet X20.

5.28.14 SNMP

The VideoJet X20 supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The unit supports SNMP MIB II in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target units here.
If you select **On** for the **SNMP** parameter and do not enter an SNMP host address, the VideoJet X20 does not send them automatically, but only replies to SNMP requests. If you enter one or two SNMP host addresses, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

5.28.15 1. SNMP host address / 2. SNMP host address

If you wish to send SNMP traps automatically, enter the IP addresses of one or two required target units here.

5.28.16 SNMP traps

You can select which traps are to be sent.

1. Click **Select**. A new window will open.
2. Click the checkboxes to select the required traps. All the checked traps will be sent.
3. Click **OK** to apply the selection.

5.28.17 Authentication

If a RADIUS server is employed in the network for managing access rights, authentication must be activated here to allow communication with the unit. The RADIUS server must also contain the corresponding data.
To configure the unit, you must connect the VideoJet X20 directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated.

5.28.18 Identity

Enter the name that the RADIUS server is to use for identifying the VideoJet X20.

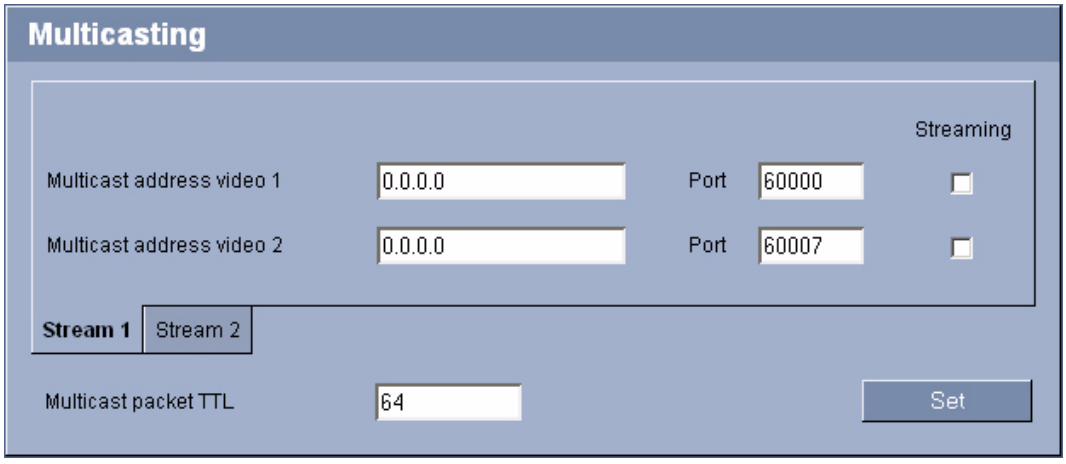
5.28.19 Password

Enter the password that is stored in the RADIUS server.

5.28.20 Automatic IP assignment

If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the VideoJet X20.
Certain applications (VIDOS, Bosch Video Management System, Archive Player, Configuration Manager) use the IP address for the unique allocation of the unit. When using such applications, the DHCP server must support the allocation of static IP addresses based on MAC addresses and must be configured accordingly, so that the unit receives the same IP address after each restart.

5.29 Multicasting



In addition to a 1:1 connection between an encoder and a single receiver (unicast), the VideoJet X20 can enable multiple receivers to receive the video signal from an encoder simultaneously. The unit either duplicates the data stream itself and then distributes it to multiple receivers (multi-unicast) or it sends a single data stream to the network, where the data stream is simultaneously distributed to multiple receivers in a defined group (multicast). For each encoder (video input) you can enter a dedicated multicast address and port for each stream. You can switch between the streams by clicking the appropriate tabs.

NOTICE!
Multicast operation requires a multicast-enabled network that uses the UDP and the Internet Group Management IGMP protocols. Other group management protocols are not supported. The TCP protocol does not support multicast connections.

A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network.
The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255.
The multicast address can be the same for multiple streams. However, it will be necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and multicast address.

NOTICE!
You must set the parameters for each encoder (video input) and for each stream individually. The numbering follows the labeling of the video inputs on the actual unit.

5.29.1 Multicast address video 1 / Multicast address video 2

Enter a valid multicast address for each stream from the relevant encoder (video input) to be operated in multicast mode (duplication of the data streams in the network).
With the setting **0.0.0.0** the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in the unit). The VideoJet X20 supports multi-unicast connections for up to five simultaneously connected receivers.

NOTICE!
Duplication of data places a heavy demand on the unit and can lead to impairment of the image quality under certain circumstances.

5.29.2 Port

Assign a different port to each data stream if there are simultaneous data streams at the same multicast address.
Enter the port address of the required stream here.

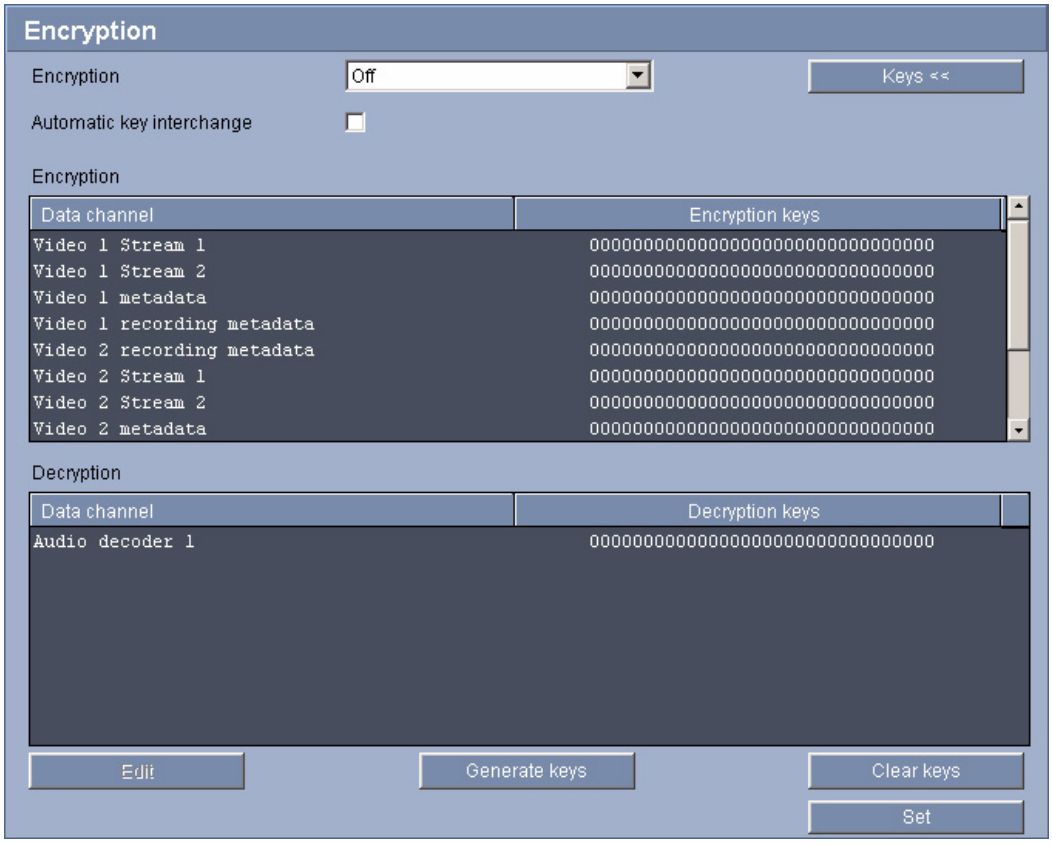
5.29.3 Streaming

Click the checkbox to activate multicast streaming mode for the relevant stream. An enabled stream is indicated by a check mark.

5.29.4 Multicast packet TTL

You can enter a value to specify how long the multicast data packets are active on the network. This value must be greater than one if multicast is to be run via a router.

5.30 Encryption



A special license, with which you will receive a corresponding activation key, is required to encrypt user data. You can enter the activation key to release the function on the **Licenses** page (see *Section 5.34 Licenses*, page 88).
Here you can activate encryption of media data (video, audio and metadata). If you activate encryption here, the exchange of connection data (RCP+) is also automatically encrypted.

CAUTION!
If you want to work with encrypted data transmission, you should allow only secured Web browser connections with SSL encryption. This is done by deactivating all open ports and protocols (see *Section 5.28 Network*, page 76).
Connections will then only be possible via the HTTPS port.

You have the option of selecting individual data channels for the encryption. As soon as a key has been generated, the data for the corresponding channel is transmitted only if encrypted. If you delete a key, the data for this channel will be transferred unencrypted.

NOTICE!
The encryption of video data requires increased computing power.

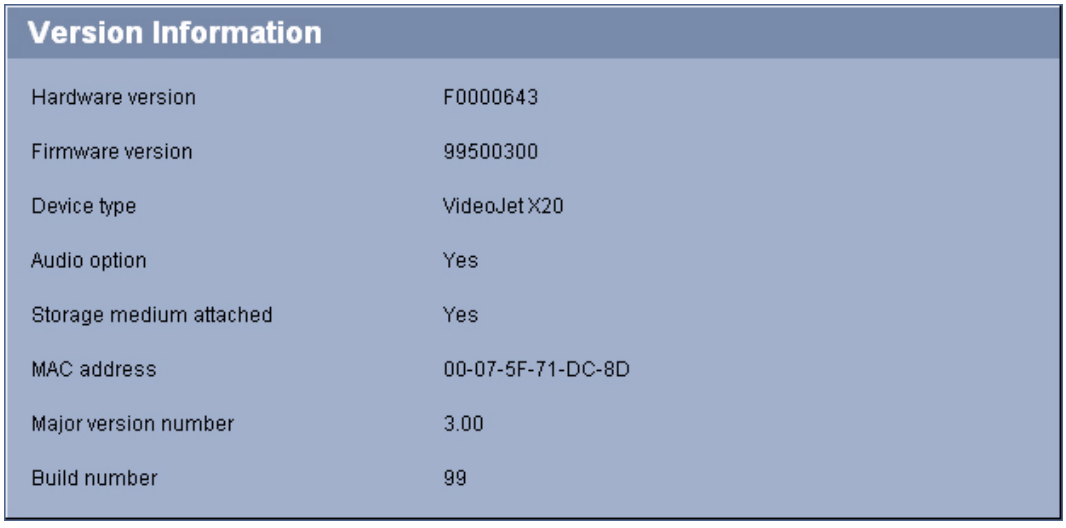
5.30.1 Encryption

1. From the **Encryption** list field, select the **On** option to activate the encryption. Keys will then be generated for all data channels.
2. Click the **Keys >>** button. The keys for the individual data channels will be displayed.
3. Click an entry in the list to select it.
4. Hold the [Ctrl] key down to select multiple entries.
5. Click the **Clear keys** button to delete the selected key. The data for this channel will now be transmitted unencrypted.
6. Click the **Generate keys** button to generate a new key for a selected channel.
7. Click the **Edit** button to enter a key for a selected entry yourself.

5.30.2 Automatic key interchange

You can activate automatic key interchange between two units (or unit and software decoder) over a secure connection. If the box is checked, keys will be automatically exchanged.

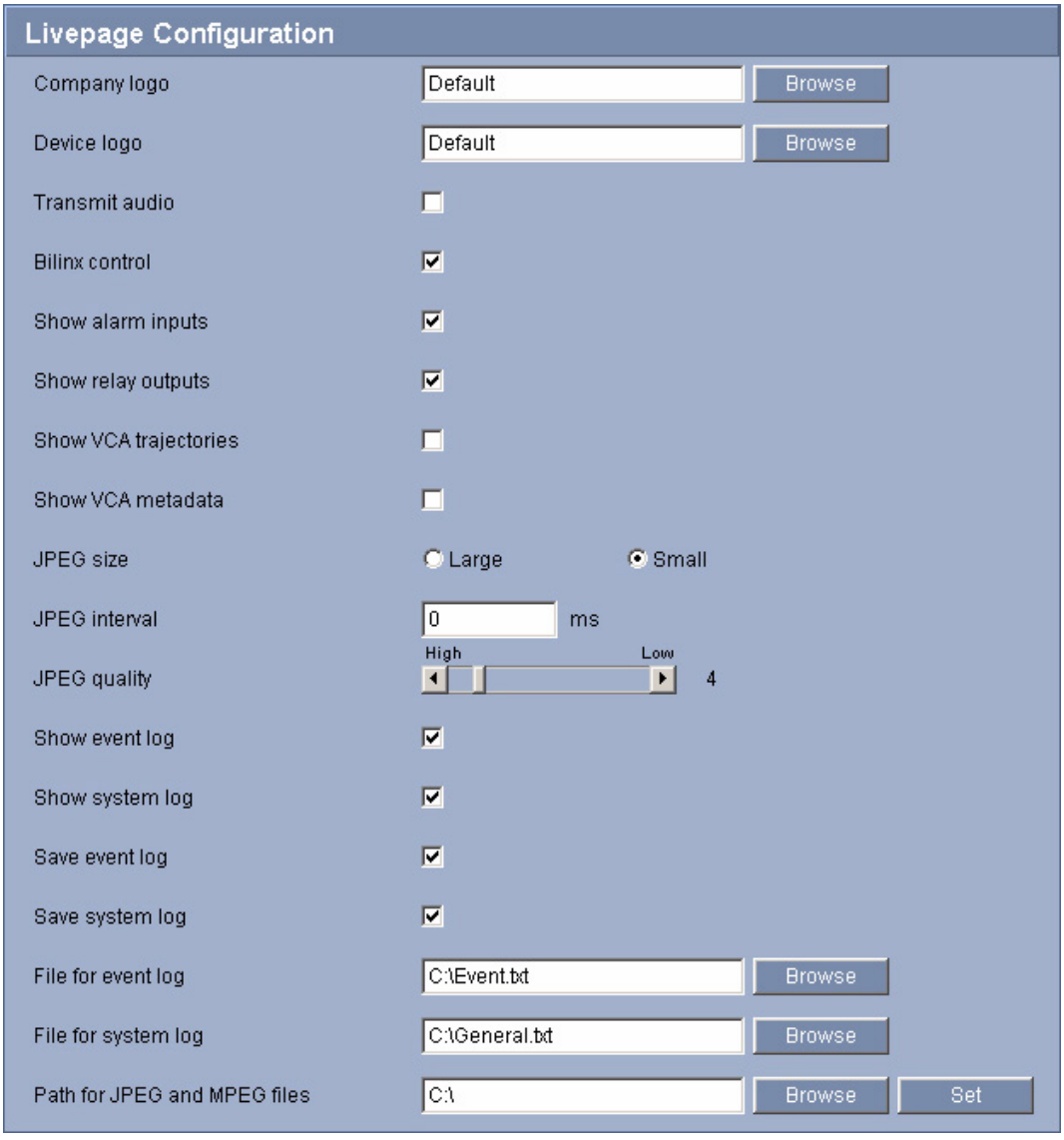
5.31 Version Information



The data on this page are for information purposes only and cannot be changed. Keep a record of this information in case technical assistance is required.

NOTICE!
You can select all required text on this page with the mouse and copy it to the clipboard with the [Ctrl]+[C] key combination, for example if you want to send it via e-mail.

5.32 Livepage Configuration



In this window you can customize the appearance of the **LIVEPAGE** to suit your requirements. You can opt to have selected information and controls displayed in addition to the video image.
If necessary, you can also replace the manufacturer's logo (top right) and the product name (top left) in the top part of the window with individual graphics.

NOTICE!
You can use either GIF or JPEG images. The file paths must correspond to the access mode (for example **C:\Images\Logo.gif** for access to local files, or **http://www.mycompany.com/images/logo.gif** for access via the Internet/Intranet).
When accessing via the Internet/Intranet, ensure that a connection is always available to display the image. The image file is not stored in the VideoJet X20.

1. Check the box for the items that are to be displayed on the **LIVEPAGE**. The selected items are indicated by a check mark.
2. Go to the **LIVEPAGE** to check whether and how the required items are displayed.

5.32.1 Company logo

1. Enter the path to a suitable graphic if you want to replace the manufacturer's logo. The image file can be stored on a local computer, in the local network or at an Internet address.
2. If necessary, click **Browse** to search for an appropriate graphic in the local network.

5.32.2 Device logo

1. Enter the path to a suitable graphic if you want to replace the product name. The image file can be stored on a local computer, in the local network or at an Internet address.
2. If necessary, click **Browse** to search for an appropriate graphic in the local network.

NOTICE!
If you want to use the original graphics again, simply delete the entries in the **Company logo** and **Device logo** fields.

5.32.3 Transmit audio

The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approx. 80 kbps for each connection.

5.32.4 Bilinx control

Next to the field for view control at the top left of the **LIVEPAGE**, an additional field is displayed for the special Bosch Security Systems Bilinx control.

5.32.5 Show alarm inputs

The alarm inputs are shown next to the video image as icons, along with their assigned names. If an alarm is active, the corresponding icon changes color.

5.32.6 Show relay outputs

The relay outputs are shown next to the video image as icons, along with their assigned names. If the relay is switched, the icon changes color.

5.32.7 Show VCA trajectories

The trajectories (motion lines of objects) from the video content analysis are displayed in the live video image if a corresponding analysis type is activated (see *Section 5.23 VCA*, page 64).

5.32.8 Show VCA metadata

When the analysis function is activated, the additional information from the video content analysis (VCA) will be displayed in the live video image (see *Section 5.23 VCA*, page 64). With the **MOTION+** analysis type, for example, the sensor fields in which motion is recorded will be marked with rectangles.

5.32.9 JPEG size

You can choose between two given image sizes to display the M-JPEG image.

5.32.10 JPEG interval

You can specify the interval at which the individual images should be generated for the M-JPEG image.

5.32.11 JPEG quality

You can specify the image quality for displaying M-JPEG on the **LIVEPAGE**.

5.32.12 Show event log

The event messages are displayed along with the date and time in a field next to the video image.

5.32.13 Show system log

The system messages are displayed along with the date and time in a field next to the video image and provide information about establishing and ending connections, for example.

5.32.14 Save event log

Check this option to save event messages in a text file on your local computer.
You can then view, edit and print this file with any text editor or the standard Office software.

5.32.15 Save system log

Check this option to save system messages in a text file on your local computer.
You can then view, edit and print this file with any text editor or the standard Office software.

5.32.16 File for event log

1. Enter the path for saving the event log here.
2. If necessary, click **Browse** to find a suitable directory.

5.32.17 File for system log

1. Enter the path for saving the system log here.
2. If necessary, click **Browse** to find a suitable directory.

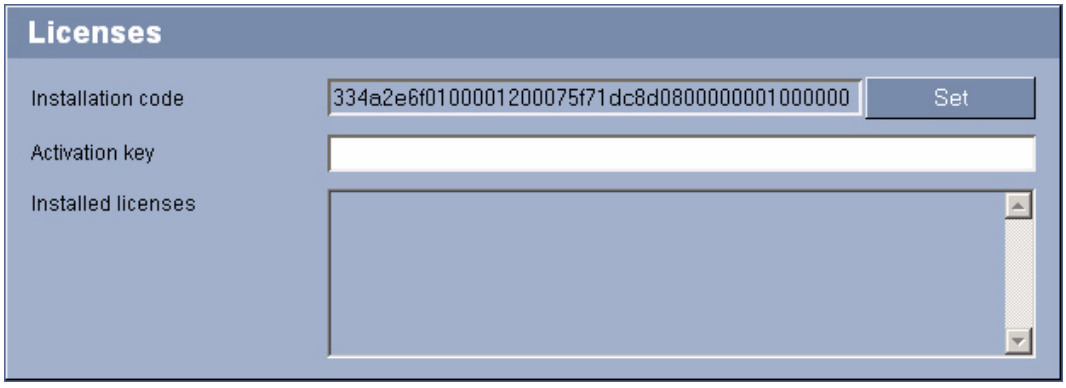
5.32.18 Path for JPEG and MPEG files

1. Enter the path for the storage location of individual images and video sequences that you can save from the **LIVEPAGE**.
2. If necessary, click **Browse** to find a suitable directory.

5.33 System State

The storage devices used by VideoJet X20 are monitored. If a storage device is no longer available for recordings, for example due to a technical defect, a **Failed** message will be displayed in this window. You can reset the error message to establish whether the error still exists.

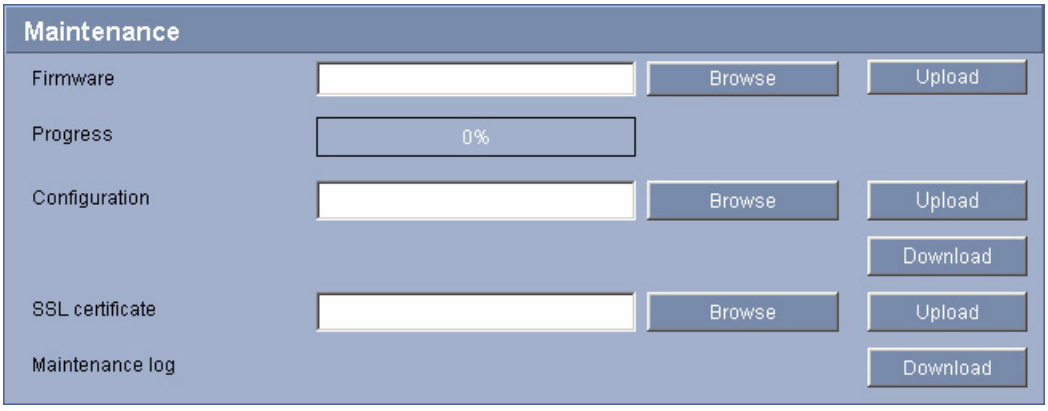
5.34 Licenses



You can enter the activation key to enable additional functions or software modules in this window.

NOTICE!
The activation key cannot be deactivated again and is not transferable to other units.

5.35 Maintenance



5.35.1 Firmware

The VideoJet X20 is designed in such a way that its functions and parameters can be updated with firmware. To do this, transfer the current firmware package to the unit via the selected network. It will then be automatically installed there.
In this way, a VideoJet X20 can be serviced and updated remotely without a technician having to change the installation on site.
You obtain the current firmware from your customer service or from the download area on our Internet site.

CAUTION!

Before launching the firmware upload make sure that you have selected the correct upload file. Uploading the wrong files can result in the unit no longer being addressable, in which case you must replace the unit.
You should never interrupt the installation of firmware. An interruption can lead to the Flash EPROM being incorrectly programmed. This in turn can result in the unit no longer being addressable, in which case it will have to be replaced. Even changing to another page or closing the browser window leads to an interruption.

1. First store the firmware file on your hard drive.
2. Enter the full path of the firmware file in the field or click **Browse** to locate and select the file.
3. Next, click **Upload** to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

The new firmware is unpacked and the Flash EPROM is reprogrammed. The time remaining is shown by the message **going to reset Reconnecting in ... seconds**. The unit reboots automatically once the upload has successfully completed.
If the **Connect** LED lights up red, the upload has failed and must be repeated. To perform the upload you must now switch to a special page:

1. In the address bar of your browser, enter **/main.htm** after the IP address of the VideoJet X20 (for example **192.168.0.20/main.htm**).
2. Repeat the upload.

5.35.2 Configuration

You can save configuration data for the VideoJet X20 on a computer and then load saved configuration data from a computer to the unit.

Upload

1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Make certain that the file to be loaded comes from the same unit type as the unit you want to configure.
3. Next, click **Upload** to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

Once the upload is complete the new configuration is activated. The time remaining is shown by the message **going to reset Reconnecting in ... seconds**. The unit reboots automatically once the upload has successfully completed.

Download

1. Click the **Download** button. A dialog box opens.
2. Follow the on-screen instructions to save the current settings.

5.35.3 SSL certificate

To be able to work with an SSL encrypted data connection, both ends of a connection must hold the relevant certificates. You can upload the SSL certificate, comprising one or multiple files, onto the VideoJet X20.

If you wish to upload multiple files onto the VideoJet X20, you must select them consecutively.

1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Next, click **Upload** to begin transferring the file to the unit.
3. Once all files have been successfully uploaded, the unit must be rebooted. In the address field of the browser, enter **/reset** after the VideoJet X20's IP address (for example **192.168.0.20/reset**).

The new SSL certificate is valid.

5.35.4 Maintenance log

You can download an internal maintenance log from the unit to send it to Customer Service for support purposes. Click **Download** and select a storage location for the file.

5.36 Function Test

The VideoJet X20 offers a variety of configuration options. You should therefore check that it is functioning correctly after installation and configuration.
The function test is the only way to ensure that the VideoJet X20 operates as expected in the event of an alarm.
Your check should include the following functions:

- Can the VideoJet X20 be called up remotely?
- Does the VideoJet X20 transmit all the required data?
- Does the VideoJet X20 respond to alarm events as required?
- Do the recordings occur as intended?
- Is it possible to control peripherals if necessary?

6 Operation

6.1 Operation with Microsoft Internet Explorer

A computer with Microsoft Internet Explorer (version 6.0 or higher) can receive live images from the VideoJet X20, control cameras or other peripherals and replay saved video sequences.

6.1.1 System Requirements

- Computer with Windows 2000 or Windows XP operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 6.0 or higher)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM
- For playing back recordings: connection to storage medium

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

6.1.2 Installing MPEG ActiveX

To allow the live video images to be played back, suitable MPEG ActiveX software must be installed on the computer. If necessary, you can install the program from the product CD supplied.

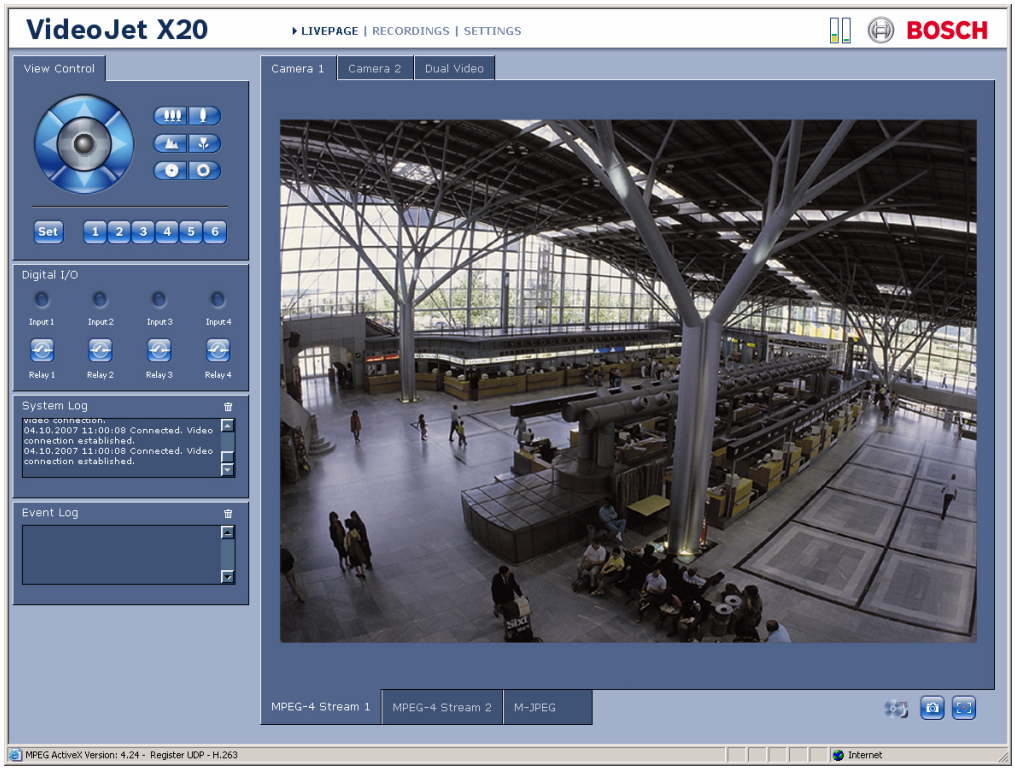
1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

6.1.3 Establishing the Connection

The VideoJet X20 must be assigned a valid IP address to operate on your network.

The following default address is preset at the factory: **192.168.0.1**

1. Start the Web browser.
2. Enter the VideoJet X20's IP address as the URL. The connection is established and after a short time you will see the **LIVEPAGE** with the video image.



6.2 The LIVEPAGE

Once the connection is established, the Web browser displays the **LIVEPAGE**. It displays the live video image on the right of the browser window. Depending on the configuration, various text overlays may be visible on the live video image (see *Section 5.5 Display Stamping*, page 32).
Other information may be shown next to the live video image on the **LIVEPAGE.** The display depends on the settings on the **Livepage Configuration** page (see *Section 5.32 Livepage Configuration*, page 85).

6.2.1 Maximum Number of Connections

If you do not connect, the unit may have reached its maximum number of connections. Depending on the unit and network configuration, each VideoJet X20 can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

6.2.2 Protected VideoJet X20

If the VideoJet X20 is password protected against unauthorized access, the Web browser displays a corresponding message and prompts you to enter the password when you attempt to access protected areas.

NOTICE!
A VideoJet X20 offers the option to limit the extent of access using various authorization levels (see *Section 5.6 Password*, page 34).

1. Enter the user name and associated password in the corresponding text fields.
2. Click **OK**. If the password is entered correctly, the Web browser displays the page that was called up.

6.2.3 Protected Network

If a RADIUS server is employed in the network for managing access rights (802.1x authentication), the VideoJet X20 must be configured accordingly, otherwise no communication is possible (see *Section 5.28.17 Authentication*, page 79).

6.2.4 Image Selection

You can view the image from each camera separately on a full screen. Alternatively, you can display the camera images from both video inputs side by side (**Dual Video**).

1. Click one of the tabs above the video image to view one or both of the camera images.
2. Click one of the tabs **MPEG-4 Stream 1**, **MPEG-4 Stream 2** or **M-JPEG** below the video image to toggle between the different displays of the camera image. The selection applies to both camera images.

6.2.5 View Control

Control options for peripherals (for example a pan/tilt camera head or dome camera) depend on the type of unit installed and on the VideoJet X20's configuration.
If a controllable unit is configured and connected to the VideoJet X20, the controls for the peripheral are displayed next to the video image.

1. To control a peripheral, click the appropriate controls.
2. Move the mouse cursor over the video image. Additional options for controlling peripherals are displayed with the mouse cursor.

6.2.6 Digital I/O

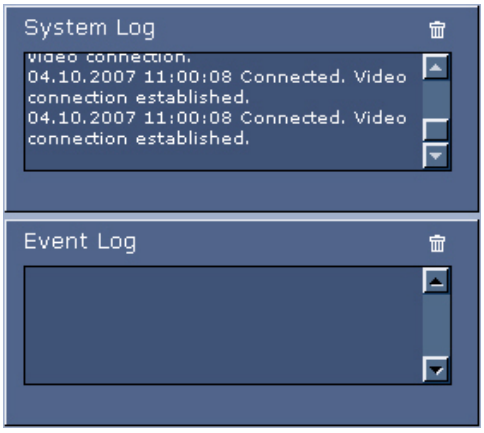
The alarm icons **Input 1** to **Input 4** are for information purposes and indicate the status of an alarm input: When an alarm is triggered, the corresponding icon lights up blue. The unit's configuration determines whether the alarm is displayed, as well as additional details (see *Section 5.32 Livepage Configuration*, page 85).

6.2.7 Trigger Relay

You can switch connected units using the relays in the VideoJet X20 (for example lights or door openers).

▶ To activate this, click the icon for the corresponding relay next to the video image. The icon will be red when the relay is activated.

6.2.8 System Log / Event Log



The **System Log** field contains information about the operating status of the VideoJet X20 and the connection. You can save these messages automatically in a file (see *Section 5.32 Livepage Configuration*, page 85).
Events such as the triggering or end of alarms are shown in the **Event Log** field. You can save these messages automatically in a file (see *Section 5.32 Livepage Configuration*, page 85).
You can delete the entries from the fields. To do this, click the icon in the top right-hand corner of the relevant field.

6.2.9 Audio Function

Depending on the configuration, the VideoJet X20 can send and receive audio signals. All users who are connected by browsers receive the audio signals sent by the VideoJet X20. Only the user who first connected to the VideoJet X20 can send audio signals to the unit.

1. On the **LIVEPAGE**, click anywhere next to the video image to remove the focus from the ActiveX.
2. Press and hold the **F12** key to establish a voice connection with the VideoJet X20. The browser's status bar displays the message **Send Audio ON**.
3. Release the **F12** key if you no longer wish to send audio signals to the VideoJet X20. The status bar in Internet Explorer displays the message **Send Audio OFF**.

NOTICE!
When the connection maintaining voice contact with the VideoJet X20 is broken, the next user to connect to the VideoJet X20 can transmit the audio data to the VideoJet X20.

6.3 Saving Snapshots

You can save individual images from the video sequence currently shown on the **LIVEPAGE** in JPEG format on your computer's hard drive.
You can save snapshots from either of the two cameras in **Dual Video** view. The icons below the camera images apply to the left or right camera image, according to their layout.

▶ Click the icon for saving single images. The image is saved at a resolution of 704 × 576 pixels (4CIF). The storage location depends on the configuration of the VideoJet X20 (see *Section 5.32.18 Path for JPEG and MPEG files*, page 87).

6.4 Recording Video Sequences

You can save sections of the video sequence currently shown on the **LIVEPAGE** on your computer's hard drive.
You can save video sequences from either of the two cameras in the **Dual Video** view. The icons below the camera images apply to the left or right camera image, according to their layout.

1. Click the icon for recording video sequences to start recording. The storage location depends on the configuration of the VideoJet X20 (see *Section 5.32.18 Path for JPEG and MPEG files*, page 87). A red dot in the icon indicates that recording is in progress.

2. Click the icon again to stop recording.

NOTICE!
You can play back saved video sequences using the Player from Bosch Security Systems, which can be installed from the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).

6.4.1 Image Resolution

Sequences are saved at the resolution that has been preset in the configuration for the encoder (see *Section 5.11 Encoder Profile*, page 38).

6.5 Running Recording Program

The hard drive icon below the camera images on the **LIVEPAGE** changes during an automatic recording.

A moving graphic will appear to indicate a running recording. If no recording is taking place, a static icon is displayed.

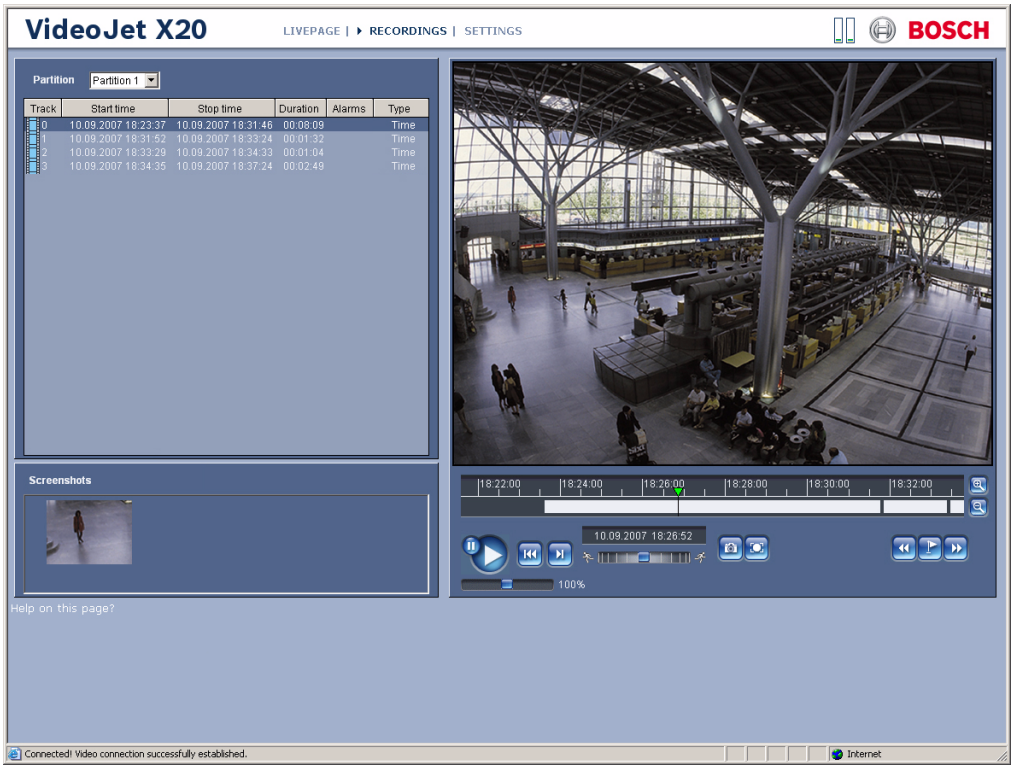
NOTICE!
You can ascertain from the **Dual Video** view for which camera a recording is running by moving the mouse cursor over the icon. A message is displayed below the mouse cursor.

6.6 The RECORDINGS Page

The **RECORDINGS** page for playing back recorded video sequences can be accessed from the **LIVEPAGE** and from the **SETTINGS** menu.

The **RECORDINGS** link is only visible if a storage medium has been selected (see *Section 5.16 Storage Medium*, page 47).

▶ Click the **RECORDINGS** link in the navigation bar in the upper section of the window. The playback page appears.

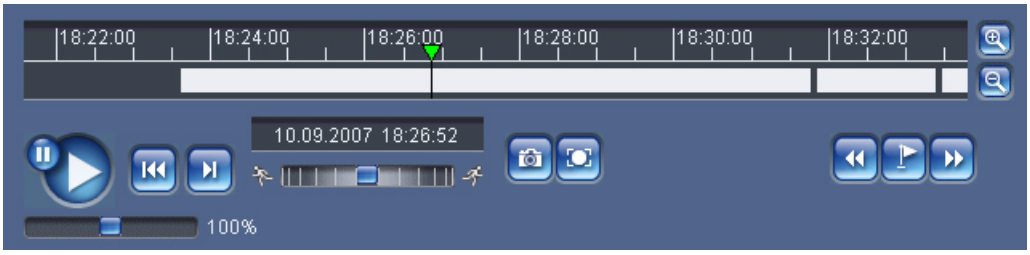


6.6.1 Selecting Recordings

In the left section of the page, first select the partition whose recordings you want to view. All sequences that are saved in the partition are displayed in the list. A running number (track) is assigned to each sequence. Start time and stop time, recording duration, number of alarms, and recording type are displayed.

1. Click a partition name from the list to display the recordings for this partition.
2. Click a list entry. The playback for the selected sequence starts immediately in the video window.

6.6.2 Controlling a Playback



You will see a time bar below the video image for quick orientation. If a particular sequence has been clicked and selected for playback, the selected sequence appears in the list in blue. The associated time interval is displayed in the bar in gray. A green arrow above the bar indicates the position of the image currently being played back within the sequence.
The time bar offers various options for navigation in and between sequences.

1. You can change the time interval displayed by moving the gray area to the left or right while holding down the mouse button.
2. You can change the time interval displayed by clicking the zoom keys (magnifying glass icons). The display can span a range from two months to a few seconds.
3. You can select a different sequence for playback by clicking the corresponding gray marking.
4. If required, drag the green arrow to the point in time at which the playback should begin. Alternatively you can click directly in the gray time interval or in the timescale to jump to the position selected in this manner. The date and time display below the bar provides orientation to the second.

6.6.3 Buttons

You can control playback by means of the buttons below the video image. The buttons have the following functions:

Start or pause playback

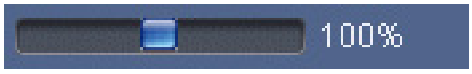
Jump to the start of the active video sequence or to the previous sequence in the list

Jump to the start of the next video sequence in the list

6.6.4 Slide Control

You can use the slide control to control playback speed and fast forward/rewind: positioning in the middle indicates playback at recording speed, left indicates rewind, and right fast forward. The fast forward or rewind speed changes, depending on how far you move the slide control toward the runner icons.

You can continuously select playback speed by means of the speed regulator:



Red bars within the gray sequence fields indicate the points in time where alarms were triggered. Drag the green arrow to navigate to these points quickly.

6.6.5 Bookmarks

In addition, you can set markers in the sequences, so-called bookmarks, and jump directly to these. These bookmarks are indicated as small yellow arrows above the time interval. Use the bookmarks as follows:

Jump to the previous bookmark

Set bookmark

Jump to the following bookmark

▶ Right-click a bookmark to delete it.

NOTICE!
Bookmarks are only valid while you are in the **RECORDINGS** page; they are not saved with the sequences. As soon as you leave the page all bookmarks are deleted.

6.7 Backup

You can back up the video sequences or single images saved on the storage medium of the VideoJet X20 to the computer's hard drive.
First select the required sequence as described in the previous section. The following buttons are available for the backup:

Back up a sequence to the computer's hard drive

Back up a single image to the computer's hard drive

1. Start playback of the sequence that you want to save either completely or partially on the computer's hard drive.
2. Click the icon for the sequence backup. The backup starts immediately — this process is displayed by a red dot in the icon.
3. Click the sequence backup icon again to end the backup.

This procedure can be repeated many times within the sequence to back up multiple extracts from a longer sequence.

▶ Click the button for backing up a single image to back up only snapshots from the running sequence to your computer's hard drive.

The single images are immediately displayed in the **Screenshots** area after clicking. The storage location for the sequences and single images can be specified in the configuration of the VideoJet X20 (see *Section 5.32.18 Path for JPEG and MPEG files*, page 87).

6.7.1 Printing a Screenshot

You can view and print the saved screenshots individually.

1. Click a preview in the **Screenshots** area. A new window will open.
2. Click the **Print** button to start the printing process.
3. Click the close button **X** in the window title bar to close the window again.

6.8 Installing the Player

You can play back saved video sequences using the Player from Bosch Security Systems, which can be found on the product CD supplied (see *Section 3.1 Scope of Delivery*, page 11).

NOTICE!
In order to play back saved sequences using the Player, suitable MPEG ActiveX software must be installed on the computer.

1. Insert the CD into the computer's CD-ROM drive. If the CD does not start automatically, open the CD in Windows Explorer and double-click the **index.html** file to start the menu.
2. From the list field at the top, select the language you require and click **Tools** in the menu.
3. Click the **Archive Player** option. The installation will start. Follow the instructions in the installation program. The Archive Player will be installed at the same time as the Player.
4. After successful installation, you will find two new icons on your desktop for the Player and the Archive Player.
5. Start the Player by double-clicking the **Player** icon.

6.9 Hardware Connections Between Video Servers

You can easily connect a VideoJet X20 with connected cameras as a sender, and a suitable MPEG-4 compatible hardware decoder (for example VIP XD) with a connected monitor as a receiver via an Ethernet network. In this way it is possible to cover long distances without the need for major installation or cabling work.

NOTICE!
The sender and receiver must be located in the same subnet to establish a hardware connection.

6.9.1 Installation

Compatible video servers are designed to connect to one another automatically, provided they are correctly configured. They only need to be part of a closed network. Proceed as follows to install the units:

1. Connect the units to the closed network using Ethernet cables.
2. Connect them to the power supply.

NOTICE!
Make sure that the units are configured for the network environment and that the correct IP address for the remote location to be contacted in the event of an alarm is set on the **Alarm Connections** configuration page (see *Section 5.22 Alarm Connections*, page 61).

6.9.2 Connecting

There are three options for establishing a connection between a sender and a compatible receiver in a closed network:

– an alarm,
– a terminal program or
– Internet Explorer.

NOTICE!
Connecting with a Web browser is described in the manual of the relevant unit that is to be used as the receiver, for example VIP XD.

6.9.3 Connecting on Alarm

With the appropriate configuration, a connection between a sender and a receiver is made automatically when an alarm is triggered (see *Section 5.22 Alarm Connections*, page 61). After a short time the live video image from the sender appears on the connected monitor.
This option can also be used to connect a sender and a compatible receiver using a switch connected to the alarm input. You do not need a computer to make the connection in this case.

6.9.4 Connecting with a Terminal Program

Various requirements must be met in order to operate with a terminal program (see *Section 8.8 Communication with Terminal Program*, page 117).

1. Start the terminal program and enter the command **1** in the main menu to switch to the **IP** menu.
2. Enter the command **4** in the **IP** menu to change the remote IP address, then enter the IP address of the unit you wish to connect to.
3. Enter the command **0** to return to the main menu and then enter the command **4** to switch to the **Rcp+** menu.
4. In the **Rcp+** menu, enter the command **5** to activate the automatic connection.

6.9.5 Closing the Connection with a Terminal Program

1. Start the terminal program and enter the command **4** in the main menu to switch to the **Rcp+** menu.
2. In the **Rcp+** menu, enter the command **5** to deactivate the automatic connection.

6.10 Operation Using Software Decoders

The VideoJet X20 video server combines with VIDOS to provide a high-performance system solution.
VIDOS is a software package for operating, controlling and managing CCTV installations (such as surveillance systems) at remote locations. It runs under Microsoft Windows operating systems. It is primarily designed for decoding video, audio and control data received from a remote sender.
There are many options available for operation and configuration when using a VideoJet X20 with VIDOS. Please refer to the software documentation for more details.

Another program that supports the VideoJet X20 is Bosch Video Management System.
Bosch Video Management System is an IP video security solution that enables the seamless management of digital video, audio and data over any IP network. It was developed for use with Bosch CCTV products as one component of an extensive video security management system. It allows you to integrate your existing components into a simple-to-control system or into the entire Bosch range, benefiting from a complete security solution based on the latest technology and years of experience.

The VideoJet X20 video server is also designed for use with the DiBos 8 digital recorder. DiBos 8 records up to 32 video and audio streams and is available as IP software or hybrid DVR with additional analog camera and audio inputs. DiBos supports the most diverse functions on the VideoJet X20 video server, for example relay activation, remote control of peripherals and remote configuration. DiBos 8 can use the alarm inputs for event triggering and on release of the MOTION+ motion detector, record the activated cells to enable intelligent motion search.

7 Maintenance and Upgrades

7.1 Testing the Network Connection

You can use the **ping** command to check the connection between two IP addresses. This allows you to test whether a unit in the network is active.

1. Open the DOS command prompt.
2. Type **ping** followed by the IP address of the unit.

If the unit is found, the response appears as **Reply from ...** followed by the number of bytes sent and the transmission time in milliseconds. If not, the unit cannot be accessed over the network. This might be because:

– The unit is not properly connected to the network. Check the cable connections in this case.
– The unit is not correctly integrated into the network. Check the IP address, subnet mask and gateway address.

7.2 Unit Reset

You can use the Factory Reset button to restore the unit to its original settings. Any changes to the settings are overwritten by the factory defaults. A reset may be necessary, for example, if the unit has invalid settings that prevent it from functioning as desired.

CAUTION!
All configured settings will be discarded during a reset.
If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.35 Maintenance*, page 89).

NOTICE!
After a reset, the unit can only be addressed via the factory default IP address. The IP address can be changed as described in the **Installation** chapter (see *Section 4.5 Setup Using the Configuration Manager*, page 25).

1. If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.35 Maintenance*, page 89).
2. Using a pointed object, press the Factory Reset button located below the orange terminal block until the **Connect** LED flashes red (see *Section 3.4 Connections on the Front Panel*, page 16). All settings will revert to their defaults.
3. Change the IP address of the VideoJet X20 if necessary.
4. Configure the unit to meet your requirements.

7.3 Repairs

CAUTION!
Never open the VideoJet X20 housing.
The unit does not contain any user-serviceable parts.

Ensure that all maintenance or repair work is carried out only by qualified personnel (electrical engineers or network technology specialists). In case of doubt, contact your dealer's technical service center.

7.4 Transfer and Disposal

The VideoJet X20 should only be passed on together with this installation and operating manual.
Your Bosch product is designed and manufactured with high quality materials and components which can be recycled and reused.

This symbol means that electrical and electronic equipment, at their end-of-life, should be disposed of separately from your household waste.
In the European Union, there are separate collection systems for used electrical and electronic products. Please dispose of this equipment at your local community waste collection/ recycling center.

8 Appendix

8.1 Troubleshooting

If you are unable to resolve a malfunction, please contact your supplier or system integrator or go directly to Bosch Security Systems Customer Service.
You can view a range of information about your unit version on the **Version Information** page (see *Section 5.31 Version Information*, page 84). Make a note of this information before contacting Customer Service. You can download an internal maintenance log from the unit on the **Maintenance** page if you wish to send it to Customer Service by e-mail (see *Section 5.35.4 Maintenance log*, page 90).

The following tables are intended to help you identify the causes of malfunctions and correct them where possible.

8.2 General Malfunctions

Malfunction	Possible causes	Recommended solution
No connection between the unit and terminal program.	Incorrect cable connections.	Check all cables, plugs, contacts, terminals and connections.
	The computer's serial interface is not connected.	Check the other serial interface.
	Interface parameters do not match.	If necessary select a different interface and make sure that the computer's interface parameters match those of the unit. Try the following standard parameters: 19,200 baud, 8 data bits, no parity, 1 stop bit. Next, disconnect the unit from the power supply and reconnect it again after a few seconds.
No image transmission to remote station.	Camera error.	Connect local monitor to the camera and check the camera function.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
No connection established, no image transmission.	The unit's configuration.	Check all configuration parameters.
	Faulty installation.	Check all cables, plugs, contacts and connections.
	Wrong IP address.	Check the IP addresses (terminal program).
	Faulty data transmission within the LAN.	Check the data transmission with **ping**.
	The maximum number of connections has been reached.	Wait until there is a free connection and then call the sender again.
No audio transmission to remote station.	Hardware fault.	Check that all connected audio units are operating correctly.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
	Incorrect configuration.	Check audio parameters on the **Audio** configuration and **Livepage Configuration** pages.
	The audio voice connection is already in use by another receiver.	Wait until the connection is free and then call the sender again.

Malfunction	Possible causes	Recommended solution
The unit does not report an alarm.	Alarm source is not selected.	Select possible alarm sources on the **Alarm Sources** configuration page.
	No alarm response specified.	Specify the desired alarm response on the **Alarm Connections** configuration page, change the IP address if necessary.
Control of cameras or other units is not possible.	The cable connection between the serial interface and the connected unit is not correct.	Check all cable connections and ensure all plugs are properly fitted.
	The interface parameters do not match those of the other unit connected.	Make sure that the settings of all units involved are compatible.
The unit is not operational after a firmware upload.	Power failure during programming by firmware file.	Have the unit checked by Customer Service and replace if necessary.
	Incorrect firmware file.	Enter the IP address of the unit followed by **/main.htm** in your Web browser and repeat the upload.

8.3 Malfunctions with iSCSI Connections

Malfunction	Possible causes	Recommended solution
After connecting to the iSCSI destination, no LUNs are displayed.	Incorrect LUN mapping during iSCSI system configuration.	Check the iSCSI system configuration and reconnect.
After connecting to the iSCSI destination, "LUN FAIL" appears below a node.	The LUN list could not be read, as it was assigned to the wrong network interface.	Check the iSCSI system configuration and reconnect.
LUN mapping is not possible.	Some iSCSI systems do not support the use of an initiator extension.	Delete the initiator extension on the **iSCSI** configuration page.

8.4 LEDs

The VideoJet X20 network video server has a number of LEDs on its front and rear panels that show the operating status and can give indications of possible malfunctions:

8.4.1 Power On LED

Does not light up:	VideoJet X20 is switched off.
Lights up green:	VideoJet X20 is switched on.

8.4.2 SFP LED

Does not light up:	No connection.
Lights up yellow:	Connection established.
Flashes yellow:	Data being transmitted.

8.4.3 ETH 1 LED

Does not light up:	No network connection.
Lights up yellow:	Network connection established.
Flashes yellow:	Data being transmitted over the network.

8.4.4 ETH 2 LED

Does not light up:	No network connection.
Lights up yellow:	Network connection established.
Flashes yellow:	Data being transmitted over the network.

8.4.5 Connect LED

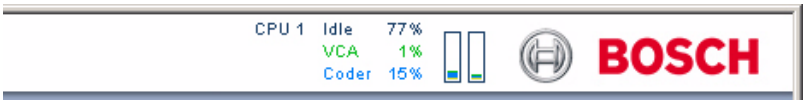
Lights up red:	Startup in progress.
Lights up green:	Startup complete, VideoJet X20 is operational.
Flashes green:	Video connection established.
Flashes red:	VideoJet X20 is faulty, for example following failed firmware upload.

8.4.6 HDD LED

Does not light up:	No hard drive fitted.
Lights up orange:	Hard drive fitted.
Flashes orange:	Hard drive activity.

8.5 Processor Load

If the VideoJet X20 is accessed via the Web browser, you will see the processor load indicators in the top left of the window next to the manufacturer's logo.



Moving the mouse cursor over one of the two graphic indicators displays the status of the corresponding processor together with the numerical values. This information may help you with troubleshooting or fine tuning the unit.

8.6 Serial Interface

Options for using the serial interface include transferring transparent data, controlling connected units or operating the unit with a terminal program.
The serial interface supports the RS232, RS422 and RS485 transmission standards. The mode used depends on the current configuration (see *Section 5.27 COM1*, page 74). Connection is via the terminal block.

8.7 Terminal Block

The terminal block has several contacts for:

– 4 alarm inputs
– 4 relay outputs
– Serial data transmission

8.7.1 Pin Assignment

The pin assignment of the serial interface depends on the interface mode used (see *Section 5.27 COM1*, page 74).

Contact	RS232 mode	RS422 mode	RS485 mode
CTS	CTS (clear to send)	RxD- (receive data minus)	Data-
TXD	TxD (transmit data)	TxD- (transmit data minus)	
RTS	RTS (ready to send)	TxD+ (transmit data plus)	Data+
RXD	RxD (receive data)	RxD+ (receive data plus)	
GND	GND (ground)	—	—

Contact	Function
IN1	Input alarm 1
IN2	Input alarm 2
IN3	Input alarm 3
IN4	Input alarm 4
GND	Ground
R1	Relay output 1
R2	Relay output 2
R3	Relay output 3
R4	Relay output 4
RM1	LED remote indicator
RM2	LED remote indicator
BP	Backup power supply
GND	Ground
+	10 to 30 V (power supply)
–	Ground

Connect each alarm input to a ground contact (GND) when connecting alarm inputs.
For the RM1 and RM2 contact specifications, see *Section 4.3.10 Remote Indication of the Connection Status*, page 23.
For the backup power supply specifications, see *Section 4.3.11 Backup Power Supply*, page 24.

8.8 Communication with Terminal Program

8.8.1 Data Terminal

If a VideoJet X20 cannot be found in the network or the connection to the network is interrupted, you can connect a data terminal to the VideoJet X20 for initial setup and setting of important parameters. The data terminal consists of a computer with a terminal program. You require a serial transmission cable with a 9-pin Sub-D plug to connect to the computer and open ends for connection to the terminal block of the VideoJet X20 (see *Section 8.7.1 Pin Assignment*, page 116).
HyperTerminal, a communications accessory included with Microsoft Windows, can be used as the terminal program.

NOTICE!
Information on installing and using HyperTerminal can be found in the manuals or in the online help for MS Windows.

1. Disconnect the VideoJet X20 from the Ethernet network before working with the terminal program.
2. Connect the serial interface of the VideoJet X20 using any available serial interface on the computer.

8.8.2 Configuring the Terminal

Before the terminal program can communicate with the VideoJet X20, the transmission parameters must be matched. Make the following settings for the terminal program:

- 19,200 bps
- 8 data bits
- No parity check
- 1 stop bit
- No protocol

8.8.3 Command Inputs

After the connection has been established, you must log onto the VideoJet X20 to access the main menu. Other submenus and functions can be accessed using the on-screen commands.

1. If necessary, turn off the local echo so that entered values are not repeated on the display.
2. Enter one command at a time.
3. When you have entered a value (such as an IP address), check the characters you have entered before pressing Enter to transfer the values to the VideoJet X20.

8.8.4 Assigning an IP Address

To use a VideoJet X20 in your network, you must assign it an IP address that is valid for your network.

The following default address is preset at the factory: **192.168.0.1**

1. Start a terminal program such as HyperTerminal.
2. Enter the user name **service**. The terminal program displays the main menu.
3. Enter command **1** to open the **IP** menu.

```
------------------------------------------------
|  VideoJet-X10_20_40
------------------------------------------------

' 0'  Exit menu IP      (* = reset after change necessary)
' 1'  local IP          (*) 192.168.0.1
' 2'  local subnet mask (*) 255.255.255.0
' 3'  local gateway     (*) 0.0.0.0
' 4'  remote IP             0.0.0.0
' 5'  ntp server            0.0.0.0
' 6'  ntp mode              1 (SNTP)
' 7'  DHCP enabled      (*) NO
' 8'  igmp version      (*) Auto
' 9'  alarm IP ...
' a'  discover ...
' b'  iscsi ...
' c'  http  port            80
' d'  https port           443
' e'  ftp server IP         0.0.0.0
' f'  syslog host IP        0.0.0.0

------------------------------------------------
```

4. Enter **1** again. The terminal program displays the current IP address and prompts you to enter a new IP address.
5. Enter the desired IP address and press Enter. The terminal program displays the new IP address.
6. Use the displayed commands for any additional settings which you require.

NOTICE!

You must reboot to activate the new IP address, a new subnet mask or a gateway address.

8.8.5 Reboot

Briefly interrupt the power supply to the VideoJet X20 for a reboot (disconnect the power supply unit from the mains supply and switch on again after a few seconds).

8.8.6 Additional Parameters

You can use the terminal program to check other basic parameters and modify them where necessary. Use the on-screen commands in the various submenus to do this.

9 Glossary

Symbols

10/100 Base-T	IEEE-802.3 specification for 10 or 100 Mbps Ethernet
802.1x	The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (*see* RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

A

ARP	Address Resolution Protocol: a protocol for mapping MAC and IP addresses

B

Baud	Unit of measure for the speed of data transmission
bps	Bits per second, the actual data rate

C

CF	CompactFlash; interface standard, for digital storage media amongst other things. Used in computers in the form of CF cards, digital cameras and Personal Digital Assistants (PDA).
CIF	Common Intermediate Format, video format with 352 × 288/240 pixels

D

DHCP	Dynamic Host Configuration Protocol: uses an appropriate server to enable dynamic assignment of an IP address and other configuration parameters to computers on a network (Internet or LAN).
DNS	Domain Name Service

F

FTP	File Transfer Protocol
Full duplex	Simultaneous data transmission in both directions (sending and receiving)

G

GBIC	GigaBit Interface Converter; applied in network technology to render interfaces flexible, for converting an electrical interface into an optical interface, for example. This enables flexible operation of an interface as a Gigabit Ethernet via twisted-pair cables or fiber optic cables.
GoP	Group of Pictures

H

HTTP	Hypertext Transfer Protocol: protocol for transmitting data over a network

HTTPS	Hypertext Transfer Protocol Secure: encrypts and authenticates communication between Web server and browser

I

ICMP	Internet Control Message Protocol
ID	Identification: a machine readable character string
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
Internet Protocol	The main protocol used on the Internet, normally in conjunction with the Transfer Control Protocol (TCP): TCP/IP
IP	*See* Internet Protocol
IP address	A 4-byte number uniquely defining each unit on the Internet. It is usually written in dotted decimal notation, for example "209.130.2.193"
iSCSI	Storage over IP process for storage networks; specifies how storage protocols are operated over IP.
ISDN	Integrated Services Digital Network

J

JPEG	An encoding process for still images (Joint Photographic Experts Group)

K

kbps	Kilobits per second, the actual data rate

L

LAN	*See* Local area network
Local area network	A communications network serving users within a limited geographical area such as a building or university campus. It is controlled by a network operating system and uses a transfer protocol.
LUN	Logical Unit Number; logical drive in iSCSI storage systems

M

MAC	Media Access Control
MIB	Management Information Base; a collection of information for remote servicing using the SNMP protocol
MPEG-4	A further development of MPEG-2 designed for transmitting audiovisual data at very low transfer rates (for example over the Internet)
MSS	Maximum Segment Size; maximum byte figure for the user data in a data packet

N

Net mask	A mask that explains which part of an IP address is the network address and which part is the host address. It is usually written in dotted decimal notation, for example "255.255.255.192"
NTP	Network Time Protocol; a standard for synchronizing computer system clocks via packet-based communication networks. NTP uses the connectionless network protocol UDP. This was developed specifically for enabling time to be reliably transmitted over networks with variable packet runtime (Ping).

O

OF	Optical Fiber; now used predominantly as the transmission medium for line-borne telecommunication processes (glass fiber cable)

P

Parameters	Values used for configuration

Q

QCIF	Quarter CIF, video format with 176 × 144/120 pixels

R

RADIUS server	Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (*see* 802.1x) and DSL.
RFC 868	A protocol for synchronizing computer clocks over the Internet
RS232/RS422/RS485	Standards for serial data transmission
RTP	Realtime Transport Protocol; a transfer protocol for real-time video and audio

S

SFP	Small Form-factor Pluggable; small, standardized module for network connections, designed as a plug connector for high-speed network connections
SNIA	Storage Networking Industry Association; association of companies for defining the iSCSI standard
SNMP	Simple Network Management Protocol; a protocol for network management, for managing and monitoring network components
SNTP	Simple Network Time Protocol; a simplified version of NTP (*see* NTP)
SSL	Secure Sockets Layer; an encryption protocol for data transmission in IP-based networks
Subnet mask	*See* Net mask

T

TCP	Transfer Control Protocol
Telnet	Login protocol with which users can access a remote computer (Host) on the Internet
TLS	Transport Layer Security; TLS 1.0 and 1.1 are the standard advanced developments of SSL 3.0 (*see* SSL)
TTL	Time-To-Live; life cycle of a data packet in station transfers

U

UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair

W

WAN	*See* Wide area network
Wide area network	A long distance link used to extend or connect remotely located local area networks

10 Specifications

10.1 Unit

Operating voltage	10 to 30 V DC, power supply via external unit
Power consumption	Approx. 22 VA with full equipment
LAN interfaces	2 × Ethernet 10/100 Base-T, automatic adjustment, half/full duplex, RJ45
Data interfaces	1 × RS232/RS422/RS485, bidirectional, push-in terminal 2 × USB 2.0, max. 2.5 W each
SFP slot	1 × 1 Gbps, for mini-GBIC modules
CF slot	1 × CompactFlash type I and II, for standard CF cards
RAM memory	8 MB per channel
Alarm inputs	4 × push-in terminals (non-isolated closing contact), maximum activation resistance 10 Ohm
Relay outputs	4 × push-in terminal, 30 V_{p-p}, 2 A, 8 contacts
Video inputs	1 × BNC socket 0.7 to 1.2 V_{p-p}, 75 Ohm, PAL/NTSC
Audio input (Line In)	1 × 3.5 mm stereo socket 5.5 V_{p-p} max., impedance 9 kOhm typ.
Audio output (Line Out)	1 × 3.5 mm stereo socket, 3.0 V_{p-p} max. at impedance 10 kOhm typ., 1.7 V_{p-p} max. at impedance 16 Ohm typ.
Displays	2 × LED (video link, hard drive) on front panel, 4 × LED (operating voltage, 2 × network connection, SFP connection) on rear panel
Thermal value	75 BTU/h with full equipment
Operating conditions	Temperature: –30 to +60 °C / –22 to +140 °F relative humidity: 0 to 95%, non-condensing
Approvals	IEC 60950; UL 60950; AS/NZS 3548 Class B; EN 50130-4; EN 50121-4; EN 55103-1; EN 55022; EN 55024; EN 60068-2-1 Ab; EN 60068-2-2 Bb; EN 60068-2-6 Fc; EN 60068-2-14 Na; EN 60068-2-30 Db; EN 61000-3-2; EN 61000-3-3; FCC 47 CFR Chapter 1 Part 15
Dimensions (H × W × D)	61 × 160 × 178 mm / 2.4 × 6.3 × 7.0 in, including BNC connections
Weight	Approx. 1.5 kg / 3.3 lb, including HDD

10.2 Protocols/Standards

Video standards	PAL, NTSC
Video coding protocols	MPEG-4, M-JPEG, JPEG
Video data rate	9.6 kbps to 6 Mbps
Image resolutions (PAL/NTSC)	704 × 576/480 pixels (4CIF/D1) 704 × 288/240 pixels (2CIF) 464 × 576/480 pixels (2/3 D1) 352 × 576/480 pixels (1/2 D1) 352 × 288/240 pixels (CIF) 176 × 144/120 pixels (QCIF)
Total delay	120 ms (PAL/NTSC, MPEG-4, no network delay)
Image refresh rate	25/30 ips max.
Network protocols	RTP, Telnet, UDP, TCP, IP, HTTP, HTTPS, DHCP, IGMP V2, IGMP V3, ICMP, ARP, SNTP, SNMP (V1/V2c/V3 MIB-II), 802.1x
Audio coding protocol	G.711, 300 Hz to 3.4 kHz
Audio sampling rate	8 kHz
Audio data rate	80 kbps

11 Index

A
Activating the recording 59
Activation key 88
Actuator 22
Alarm 17, 32, 96
Alarm e-mail 69
Alarm input 22
Alarm message 33
Alarm sensors 57
Alarm sources 60
Alarm track recording 57
Alarm track size 55
Alarm tracks 55
Audio connections 16, 20
Audio input 16
Audio output 16
Audio settings 44
Audio source selection 44
Audio stream on alarm 63
Audio transmission 86
Auto-connect 63
Automatic key interchange 83

B
Backup 103
Baud rate 75
Bookmarks 102
Brightness 37
Browser window 95

C
Camera 75
Camera name 31
Camera selection 95
Cameras 20
Car battery 24
CF card 17, 21
Changes 30, 53
Changes in light level 65
Checking network 109
COM1 74
CompactFlash 17, 21
Configuration 27, 90
Configuration download 90
Configuration mode 29
Connecting 27, 105
Connecting on alarm 61
Continuous recording 57
Contrast 37
Control 74
Control functions 96
Controlling a playback 101
Conventions 7
Creating a partition 52

D
Danger 9
Data bits 75
Data interface 22
Data terminal 117
Date 35
Date format 35
Daylight saving time 36
Default 41
Default camera 63
Default profile 41
Defaults 56, 64
Deleting recordings 55
Display stamping 32
Dome camera 22
Dual Streaming 13, 38

E
Echo 117
Editing a partition 54
Electromagnetic compatibility 8
E-mail 69
Encoder 57
Encoding 13
Encryption 82
Encryption protocol 78
EPROM 89
Establishing the connection 28, 94
Event log 87, 97

F
False alarms 65
Firewall 62, 77
Firmware upload 89
Format 55
Front panel connections 16
FTP server 45, 46
Function test 91

G
Gateway 77
GBIC module 17
General password 62

H
Holidays 59
HTTP port 77
HTTPS port 78

I
Identification 8, 31
IEEE 802.1x 79
IGMP 80
Image quality 81
Image resolution 98
Image selection 95
Installation 9
Installation conditions 19
Installation location 19
Interface 115
Interface mode 75
Internal clock 35
IP address 77, 118
iSCSI settings 48

J
JPEG format 45
JPEG posting 45
JPEG posting interval 46

L
Language 35

Licenses 88
Linear mode 54, 55
Live video images 27, 93
Livepage 85
Low Voltage Directive 8
Low-pass filter 37

M

Main functions 15
Maintenance 9
Make contact 22
Manufacturer logo 85
Media playback 100
Motion detector 64
Motion detector defaults 64
Motion detector object size 66
Motion detector sensitivity 66
MPEG ActiveX 27, 93, 104
MPEG-4 encoder 38
MTU value 77, 78
Multicast address 81
Multicast connection 77, 80
Multicast function 13
Multicasting 80
Multi-unicast 80

N

Navigation 30
Network 20, 76
Network connection 17, 25
Number of connections 28, 95

O

OF 21
Operation 9, 93
Overview of functions 13

P

Parameters 26, 118
Parity check 75
Partition 51
Partition status 53
Partitioning 51
Password 29, 34, 95
Peripheral control 96
Picture settings 37
Pin assignment 116
Playback 100
Playback button 101
Player 104
Port 77, 81
Post-alarm profile 57
Post-alarm time 57
Power off 25
Power on 25
Power supply 9, 17, 25
Power switch 25
Processor load 115
Processor load indicator 115
Product name 85
Profile configuration 40
Profiles 38
Protocol 75

R

RADIUS 79
Rear panel connections 17
Reboot 26, 118
Receiver 13
Receiver password 62
Recording profiles 56
Recording program 99
Recording scheduler 58
Recording status 59
Recording video sequences 98
Reflections of light 65
Regulations 7
Relay 17, 23
Relay output 72
Relay outputs 23
Remote control 14
Remote indication 23
Remote LED 23
Repair 9, 110
Reset 17, 109
Ring mode 54, 55
Router 81

S

Safety 9
Saturation 37
Saving event log 87
Saving system log 87
Scope of delivery 11
Screen resolution 12, 27, 93
Select area 66, 67, 68
Selecting a profile 38
Sensor fields 66, 68
Serial Interface 17
Serial number 8
Serial port function 74
SFP 17, 21
Signal source 22
SMS 69
Snapshots 14, 98
SNMP 79
SNTP server 36
Software decoder 107
Source type 43
SSL certificate 90
SSL encryption 63
Standard profile 57
Standard recording profile values 56
Stop bits 75
Storage information 47, 50
Storage medium 47
Streaming 81
Subnet mask 77
Summer time 36
Symbols 7
Synchronize 35
System log 87, 97
System requirements 12, 27, 93

T

Tamper detection 66
Target data rate 41

TCP 62, 77
Terminal 74
Termination 43
Test 91
Time 24, 32, 35
Time server 35
Time server IP address 36
Time server protocol 35
Time signal 35
Time zone 36
TLS 78
Transfer protocol 62, 77
Transmission parameters 117
Transmission rate 75
Transmission standards 22, 115
Transparent 74
Traps 79
Trigger relay 73
TTL 81

U

UDP 62, 77
Unicast 80
Unit date 35
Unit ID 31
Unit identification 31
Unit name 31
Unit reset 109
Unit time 35
URL 28, 94
USB interface 16
User name 34

V

VCR 43
Video content analysis 64
Video input 16, 43
Video sensor 64

W

Watermarking 33

Bosch Security Systems
Robert-Koch-Straße 100
D-85521 Ottobrunn
Germany
Telefon 089 6290-0
Fax 089 6290-1020
www.bosch-securitysystems.com
© Bosch Security Systems, 2007